COBIT®

5

Modelo Corporativo para Governança e Gestão de TI da Organização

COBIT® 5

AN ISACA® FRAMEWORK

ISACA®

Com 95.000 usuários em 160 países, a ISACA (www.isaca.org) é líder mundial no fornecimento de conhecimento, certificações, comunidade, advocacia e treinamento em garantia e segurança de sistemas de informação (SI), governança corporativa e gestão de TI, bem como risco e conformidade de TI. Fundada em 1969, a ISACA é uma entidade independente e sem fins lucrativos que organiza conferências internacionais, publica o ISACA® Journal e desenvolve padrões internacionais de controle e auditoria de SI que ajudam seus usuários a garantir a confiança e o valor dos sistemas de informação. Ela também antecipa e atesta conhecimento e habilidades de TI através das designações mundialmente respeitadas Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) e Certified in Risk and Information Systems Control™ (CRISC™). A ISACA atualiza continuamente o COBIT®, o que ajuda os profissionais de TI e os líderes das organizações a cumprirem suas responsabilidades de gestão e governança de TI, especialmente nas áreas de garantia, segurança, risco e controle, além de criarem valor para a organização.

Aviso Legal

A ISACA desenvolveu esta publicação, o COBIT® 5 (a 'Obra'), principalmente como um recurso educacional para profissionais de segurança, risco, garantia e governança de TI da organização (GEIT – Goverance of Enterprise IT). A ISACA não faz nenhuma afirmação de que o uso de qualquer parte da Obra garantirá um resultado positivo. A Obra não deve ser considerada de modo a incluir todas as informações, procedimentos e testes adequados ou excluir outras informações, procedimentos e testes razoavelmente voltados à obtenção dos mesmos resultados. Ao determinar a adequação de qualquer informação, procedimento ou teste específico, os leitores deverão aplicar seu próprio julgamento profissional às circunstâncias de segurança, risco, garantia e GEIT específicas apresentadas pelos sistemas ou ambientes de tecnologia da informação específicos.

Copyright

Quality Statement:

This Work is translated into Brazilian Portuguese from the English language version of COBIT® 5 Business Framework by the ISACA® Sao Paulo Chapter with the permission of ISACA®. The ISACA® Sao Paulo Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

Copyright

Disclaimer:

ISACA has designed this publication, COBIT® 5 (the "Work"), primarily as an educational resource for governance of enterprise IT (GEIT), assurance, risk and security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, readers should apply their own professional judgment to the specific GEIT, assurance, risk and security circumstances presented by the particular systems or information technology environment.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EUA Tel: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: info@isaca.org

Website: www.isaca.org
Feedback: www.isaca.org/cobit
Participe do ISACA Knowledge Center: www.isaca.org/knowledge-center
Siga o ISACA no Twitter: https://twitter.com/ISACANews
Participe do fórum COBIT no Twitter: #COBIT
Una-se à ISACA no LinkedIn: ISACA (Oficial), http://linkd.in/ISACAOfficial
Curta a ISACA no Facebook: www.facebook.com/ISACAHQ

COBIT® 5
ISBN 978-1-60420-284-7
Impresso nos Estados Unidos da América

AGRADECIMENTOS

A ISACA agradece as seguintes pessoas:

Força Tarefa COBIT 5 (2009–2011)

John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, EUA, Co-Presidente
Derek J. Oliver, Ph.D., CISA, CISM, CRISC, CITP, DBA, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., GB, Co-Presidente
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Austrália
Elisabeth Judit Antonsson, CISM, Nordea Bank, Suécia
Steven A. Babb, CGEIT, CRISC, BetFair, GB
Steven De Haes, Ph.D., University of Antwerp Management School, Bélgica
Peter Harrison, CGEIT, FCPA, IBM Australia Ltd., Austrália
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Áustria
Robert D. Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, EUA Erik H.J.M. Pols, CISA, CISM, Shell International-ITCI, Países Baixos
Vernon Richard Poole, CISM, CGEIT, Sapphire, GB
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, Índia

Equipe de Desenvolvimento

Floris Ampe, CISA, CGEIT, CIA, ISO 27000, PwC, Bélgica
Gert du Preez, CGEIT, PwC, Canadá
Stefanie Grijp, PwC, Bélgica
Gary Hardy, CGEIT, IT Winners, África do Sul
Bart Peeters, PwC, Bélgica
Geert Poels, Ghent University, Bélgica
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Bélgica

Participantes do Workshop

Gary Baker, CGEIT, CA, Canadá
Brian Barnier, CGEIT, CRISC, ValueBridge Advisors, EUA
Johannes Hendrik Botha, MBCS-CITP, FSM, getITright Skills Development, África do Sul
Ken Buechler, CGEIT, CRISC, PMP, Great-West Life, Canadá
Don Caniglia, CISA, CISM, CGEIT, FLMI, EUA Mark Chaplin, GB
Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii at Manoa, EUA
Mike Donahue, CISA, CISM, CGEIT, CFE, CGFM, CICA, Towson University, EUA
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Suíça
Bob Frelinger, CISA, CGEIT, Oracle Corporation, EUA James Golden, CISM, CGEIT, CRISC, CISSP, IBM, EUA
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, EUA Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Austrália
Nicole Lanza, CGEIT, IBM, EUA
Philip Le Grand, PRINCE2, Ideagen Plc, GB
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, EUA Stuart MacGregor, Real IRM Solutions (Pty) Ltd., África do Sul Christian Nissen, CISM, CGEIT, FSM, CFN People, Dinamarca
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, GB Eddy J. Schuermans, CGEIT, ESRAS bvba, Bélgica
Michael Semrau, RWE Germany, Alemanha
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Austrália
Alan Simmonds, TOGAF9, TCSA, PreterLex, GB Cathie Skoog, CISM, CGEIT, CRISC, IBM, EUA
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canadá
Roger Southgate, CISA, CISM, GB
Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, EUA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Bélgica
Greet Volders, CGEIT, Voquals N.V., Bélgica
Christopher Wilken, CISA, CGEIT, PwC, EUA
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, GB

Revisores Especializados

Mark Adler, CISA, CISM, CGEIT, CRISC, Commercial Metals Company, EUA Wole Akpose, Ph.D., CGEIT, CISSP, Morgan State University, EUA
Krzysztof Baczkiewicz, CSAM, CSOX, Eracent, Polônia
Roland Bah, CISA, MTN Cameroon, Camarões
Dave Barnett, CISSP, CSSLP, EUA
Max Blecher, CGEIT, Virtual Alliance, África do Sul
Ricardo Bria, CISA, CGEIT, CRISC, Meycor GRC, Argentina

Revisores Especializados (Cont)

Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Bélgica

Agradecimentos (Cont.)

Donna Cardall, GB
Debra Chiplin, Investors Group, Canadá
Sara Cosentino, CA, Great-West Life, Canadá
Kamal N. Dave, CISA, CISM, CGEIT, Hewlett Packard, EUA Philip de Picker, CISA, MCA, National Bank of Belgium, Bélgica Abe Deleon, CISA, IBM, EUA
Stephen Doyle, CISA, CGEIT, Department of Human Services, Austrália
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions, Inc., EUA Rafael Fabius, CISA, CRISC, Uruguai
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Suíça
Bob Frelinger, CISA, CGEIT, Oracle Corporation, EUA
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, ITIL V3 Trainer, PRINCE2, ISO/IEC 20000 Consultant, Turquia
Edson Gin, CISA, CISM, CFE, CIPP, SSCP, EUA
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, EUA
Marcelo Hector Gonzalez, CISA, CRISC, Banco Central Republic Argentina, Argentina
Erik Guldentops, University of Antwerp Management School, Bélgica Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, EUA Angelica Haverblad, CGEIT, CRISC, ITIL, Verizon Business, Suécia
Kim Haverblad, CISM, CRISC, PCI QSA, Verizon Business, Suécia
J. Winston Hayden, CISA, CISM, CGEIT, CRISC, África do Sul Eduardo Hernandez, ITIL V3, HEME Consultores, México
Jorge Hidalgo, CISA, CISM, CGEIT, ATC, Lic. Sistemas, Argentina
Michelle Hoben, Media 24, África do Sul
Linda Horosko, Great-West Life, Canadá
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants, GB Grant Irvine, Great-West Life, Canadá
Monica Jain, CGEIT, CSQA, CSSBB, Southern California Edison, EUA John E. Jasinski, CISA, CGEIT, SSBB, ITIL Expert, EUA
Masatoshi Kajimoto, CISA, CRISC, Japão
Joanna Karczewska, CISA, Polônia
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Arábia Saudita
Eddy Khoo S. K., Prudential Services Asia, Malásia
Marty King, CISA, CGEIT, CPA, Blue Cross Blue Shield NC, EUA Alan S. Koch, ITIL Expert, PMP, ASK Process Inc., EUA
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Austrália Jason D. Lannen, CISA, CISM, TurnKey IT Solutions, LLC, EUA Nicole Lanza, CGEIT, IBM, EUA
Philip Le Grand, PRINCE2, Ideagen Plc, GB
Kenny Lee, CISA, CISM, CISSP, Bank of America, EUA
Brian Lind, CISA, CISM, CRISC, Topdanmark Forsikring A/S, Dinamarca
Bjarne Lonberg, CISSP, ITIL, A.P. Moller - Maersk, Dinamarca
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., África do Sul
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, EUA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, GB Cindy Marcello, CISA, CPA, FLMI, Great-West Life & Annuity, EUA Nancy McCuaig, CISSP, Great-West Life, Canadá
John A. Mitchell, Ph.D., CISA, CGEIT, CEng, CFE, CITP, FBCS, FCIIA, QiCA, LHS Business Control, GB Makoto Miyazaki, CISA, CPA, Bank of Tokyo-Mitsubishi, UFJ Ltd., Japão
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, ITIL, Independent Consultant, Colômbia
Christian Nissen, CISM, CGEIT, FSM, ITIL Expert, CFN People, Dinamarca
Tony Noblett, CISA, CISM, CGEIT, CISSP, EUA
Ernest Pages, CISA, CGEIT, MCSE, ITIL, Sciens Consulting LLC, EUA Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, GB
Tom Patterson, CISA, CGEIT, CRISC, CPA, IBM, EUA
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, África do Sul
Andy Piper, CISA, CISM, CRISC, PRINCE2, ITIL, Barclays Bank Plc, GB
Andre Pitkowski, CGEIT, CRISC, OCTAVE, ISO27000LA, ISO31000LA, APIT Consultoria de Informatica Ltd., Brasil
Dirk Reimers, Hewlett-Packard, Alemanha
Steve Reznik, CISA, ADP, Inc., EUA
Robert Riley, CISSP, University of Notre Dame, EUA
Martin Rosenberg, Ph.D., Cloud Governance Ltd., GB
Claus Rosenquist, CISA, CISSP, Nets Holding, Dinamarca
Jeffrey Roth, CISA, CGEIT, CISSP, L-3 Communications, EUA Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District, EUA Eddy J. Schuermans, CGEIT, ESRAS bvba, Bélgica
Michael Semrau, RWE Germany, Alemanha
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Austrália
Alan Simmonds, TOGAF9, TCSA, PreterLex, GB
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canadá

Revisores Especializados (cont.)

Jennifer Smith, CISA, CIA, Salt River Pima Maricopa Indian Community, EUA

AGRADECIMENTOS (CONT.)

Marcel Sorouni, CISA, CISM, CISSP, ITIL, CCNA, MCDBA, MCSE, Bupa Australia, Austrália
Roger Southgate, CISA, CISM, GB
Mark Stacey, CISA, FCA, BG Group Plc, GB
Karen Stafford Gustin, MLIS, London Life Insurance Company, Canadá Delton Sylvester, Silver Star IT Governance Consulting, África do Sul Katalin Szenes, CISA, CISM, CGEIT, CISSP, University Obuda, Hungria Halina Tabacek, CGEIT, Oracle Americas, EUA
Nancy Thompson, CISA, CISM, CGEIT, IBM, EUA
Kazuhiro Uehara, CISA, CGEIT, CIA, Hitachi Consulting Co., Ltd., Japão
Johan van Grieken, CISA, CGEIT, CRISC, Deloitte, Bélgica
Flip van Schalkwyk, Centre for e-Innovation, Western Cape Government, África do Sul
Jinu Varghese, CISA, CISSP, ITIL, OCA, Ernst & Young, Canadá
Andre Viviers, MCSE, IT Project+, Media 24, África do Sul
Greet Volders, CGEIT, Voquals N.V., Bélgica
David Williams, CISA, Westpac, Nova Zelândia
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, GB Amanda Xu, PMP, Southern California Edison, EUA
Tichaona Zororo, CISA, CISM, CGEIT, Standard Bank, África do Sul

Conselho de Administração da ISACA

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (aposentado), EUA, Presidente Internacional
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grécia, Vice-Presidente
Gregory T. Grocholski, CISA, The Dow Chemical Co., EUA, Vice-Presidente
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Austrália, Vice-Presidente
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., Índia, Vice-Presidente
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., EUA, Vice-Presidente
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Austrália, Vice-Presidente
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (aposentado), EUA, Ex-Presidente Internacional
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Rússia, Ex-Presidente Internacional
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, GB, Conselheiro
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Conselheiro

Junta de Conhecimento

Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Presidente
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, EUA
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Cingapura
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, EUA
Jon Singleton, CISA, FCA, Auditor General of Manitoba (aposentado), Canadá
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, França

Comitê do Modelo (2009-2012)

Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, França, Presidente
Georges Ataya, CISA, CISM, CGEIT, CRISC, CISSP, Solvay Brussels School of Economics and Management, Bélgica, Ex-Vice-Presidente
Steven A. Babb, CGEIT, CRISC, BetFair, GB
Sushil Chatterji, CGEIT, Edutech Enterprises, Cingapura
Sergio Fleginsky, CISA, Akzo Nobel, Uruguai
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, EUA Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Anthony P. Noble, CISA, CCP, Viacom, EUA
Derek J. Oliver, Ph.D., CISA, CISM, CRISC, CITP, DBA, FBCS, FISM, Ravenswood Consultants Ltd., GB Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (aposentado), Canadá
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa, AG, Alemanha
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Austrália
Robert E. Stroud, CGEIT, CA Inc., EUA

Agradecimento Especial

ISACA Capítulo Los Angeles por seu apoio financeiro

Afiliadas e Patrocinadores da ISACA e do Instituto de Governança de TI® (ITGI®)

American Institute of Certified Public Accountants Commonwealth Association for Corporate Governance Inc. FIDA Inform
Information Security Forum
Institute of Management Accountants Inc. Capítulos ISACA
ITGI França
ITGI Japão
Norwich University

Agradecimentos (Cont.)

Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

Enterprise GRC Solutions Inc. Hewlett-Packard
IBM
Symantec Corp.

Reconhecimento da Tradução para a língua portuguesa

Voluntários

Jose Luis Diniz, CGEIT, ITIL Expert, - DNZ Consultoria em TI – Coordenador – Capítulo São Paulo
Edson Kowask Bezerra, CRISC - Rede Nacional de Ensino e Pesquisa (RNP) – Coordenador – Capítulo Brasília

Adriana da Silva Dian Leão
Adriano Jose da Silva Neves, CGEIT, CRISC
Alberto Fávero, CISSP, CISA, CISM
Alfred John Bacon, CISA,CISM,CRISC
Anderson Itaborahy, MSc, BB Tecnologia e Serviços
André Luis Regazzini, CISA, CISM, CGEIT
André Pitkowski, CRISC, CGEIT
Carlos Alberto Mamede Hernandes, CISA,CGEIT
Carlos Augusto da Costa Carvalho, CRISC
Carmen Ozores Fernandes, CISA, CRISC, CIA
Claudio Silva Da Cruz, CGEIT
Cristiane Menezes Silva
Cristiano Silva Borges
Diana Leite Nunes dos Santos, MSc., PMP, Ministério Público Federal (MPF/PGR)
Edgar D'Andrea, CISA, CISM
Edméa Pujol Canton
Ernani Paes De Barros, CISA,CISM
Fabiano Mariath D'Oliveira, Embrapa.
Fabio Alessandro Moreira da Silva
Fabio Penna F. Curto, CISM, CGEIT
Gustavo Henrique Verges Schmal
Gustavo Perri Galegale, CISA, CRISC
Homero De Almeida Carreiro
João Souza Neto, Ph.D., CGEIT, CRISC, COBIT5 Certified Assessor, Universidade Católica de Brasília.
José Geraldo Loureiro, CRISC, Instituto Brasileiro de Governança Pública (IBGP) .
Leandro Martins Ribeiro
Leandro Pfeifer Macedo, CRISC
Luiz Claudio Diogo Reis, CISA,CRISC
Marcelo Duarte Gouvea, CISA,CGEIT
Marcelo Silva Cunha
Marcos Semola, CISM
Napoleão Verardi Galegale, CGEIT
Orlando Tuzzolo Jr., CISM, CGEIT, CRISC
Osmir Perussi Bertão, CRISC
Paulo Sergio Pagliusi, CISM
Renato Mitsuo Wada, CISM
Ricardo Castro, CISA, CRISC
Rodrigo Hiroshi Ruiz Suzuki, CISA, CISM, CRISC
Vanessa Borges de Menezes
Wesley Vaz Silva, CISA
Wesley Vaz, MSc, CISA, Tribunal de Contas da União (TCU).

AGRADECIMENTOS (CONT.)

Apoio institucional dos capítulos brasileiros

Capítulo São Paulo
Diretoria Executiva em 2014 – 2017
André Pitkowski, CRISC, CGEIT, Presidente
Gustavo Perri Galegale, CISA, CRISC, Vice-Presidente
Rodrigo Hiroshi Ruiz Suzuki, CISA, CISM, CRISC, Diretor de Educação
Renato Mitsuo Wada, CISM, Diretor de Associados
Orlando Tuzzolo Jr., CISM, CGEIT, CRISC, Diretor de Comunicação
Adriano Jose da Silva Neves, CGEIT, CRISC, Diretor Secretário
Carlos Augusto da Costa CArvalho, CRISC, Diretor de Controladoria
Cristiane Menezes Silva, Dir. Parceria
Carmen Ozores Fernandes, CISA, CRISC, CIA, Past President

Diretoria Executiva em 2010 – 2013
Carmen Ozores Fernandes, CISA, CRISC, CIA, Presidente
Fabio Penna F. Curto, CISM, CGEIT, Vice Presidente
Rodrigo Hiroshi Ruiz Suzuki, CISA, CISM, CRISC, Diretor de Educação
Gustavo Perri Galegale, CISA, CRISC, Diretor de Associados
Fernando Nicolau Freitas, CISM, CGEIT, Diretor de Comunicação
Edméa Pujol Canton, Diretora Secretária
Cristiano Silva Borges, Diretor de Controladoria
André Luis Regazzini, CISA, CISM, CGEIT, Diretor de Parceria
Ricardo Castro, CISA, CRISC, Past President

Capítulo Brasília
Diretoria Executiva
Jose Geraldo Loureiro Rodrigues, CRISC, Presidente
Claudio Silva Da Cruz, CGEIT, Vice-Presidente
Joao Souza Neto, CGEIT,CRISC, Diretor de Educação
Diana Leite Nunes Dos Santos, Diretora de Associados
Leandro Pfeifer Macedo, CRISC, Diretor de Comunicação e Marketing
Carlos Alberto Mamede Hernandes, CISA,CGEIT, Diretor Secretário
Marcelo Silva Cunha, Tesoureiro
Edson Kowask Bezerra, CRISC, Diretor de Pesquisa
Wesley Vaz Silva, CISA, Coordenador de Certificação

Capítulo Rio de Janeiro
Diretoria Executiva
Alfred John Bacon, CISA,CISM,CRISC, Presidente
Marcos Semola, CISM, Vice-Presidente
Ernani Paes De Barros, CISA,CISM, Diretor de Educação
Marcelo Duarte Gouvea, CISA,CGEIT, Diretor de Associados
Paulo Sergio Pagliusi, CISM, Diretor de Comunicação
Luiz Claudio Diogo Reis, Sr., CISA,CRISC, Diretor Secretário
Leandro Martins Ribeiro, Diretor de Controladoria
Homero De Almeida Carreiro, Diretor Institucional
Ernani Paes De Barros, CISA,CISM, Diretor de Certificação

ÍNDICE

LISTA DE FIGURAS

COBIT 5: UM MODELO CORPORATIVO PARA A GOVERNANÇA E GESTÃO DE TI DA ORGANIZAÇÃO

A publicação COBIT 5 contém um modelo para governança e gestão de TI da organização. A publicação faz parte da família de produtos COBIT 5 como demonstrado na figura 1.

Figura - 1: Família de Produtos COBIT 5

COBIT® 5

Guias de Habilitadores do COBIT 5
COBIT® 5: Habilitador Processos
COBIT® 5: Habilitador Informação
Outros Guias de Habilitadores

Guias Profissionais do COBIT 5
COBIT® 5 Implementação
COBIT® 5 para Segurança da Informação
COBIT® 5 para Garantia (Assurance)
COBIT® 5 para Risco
Outros Guias Profissionais

Ambiente Colaborativo Online do COBIT® 5

O modelo do COBIT 5 baseia-se em cinco princípios básicos, que são cobertos detalhadamente e incluem ampla orientação sobre os habilitadores de governança e gestão de TI da organização.

A família de produtos COBIT 5 é formada pelos seguintes produtos:

- COBIT 5 (o modelo)
- Guias de habilitadores do COBIT 5, que detalham os habilitadores de governança e gestão. Eles incluem:
  - COBIT 5 Habilitador Processos
  - COBIT 5 Habilitador Informações
  - Outros guias habilitadores (ver *www.isaca.org/cobit*)
- Guias profissionais do COBIT 5, que incluem:
  - COBIT 5 Implementação
  - COBIT 5 para Segurança da Informação
  - COBIT 5 para Risco
  - COBIT 5 para Garantia *(Assurance)*
  - COBIT Programa de Avaliação
  - Outros guias profissionais (ver *www.isaca.org/cobit*)
- Um ambiente colaborativo on-line, que é disponibilizado para apoiar o uso do COBIT 5

SUMÁRIO EXECUTIVO

A informação é um recurso fundamental para todas as organizações e a tecnologia desempenha um papel significativo desde o momento que a informação é criada até o momento em que ela é destruída. A tecnologia da informação está cada vez mais avançada, tornando-se pervasiva nas organizações e nos ambientes sociais, públicos e corporativos.

Como consequência, hoje, mais do que nunca, as organizações e seus executivos se esforçam para:

- Manter informações de alta qualidade para apoiar decisões corporativas.
- Agregar valor ao negócio a partir dos investimentos em TI, ou seja, atingir os objetivos estratégicos e obter benefícios para a organização através da utilização eficiente e inovadora de TI.
- Alcançar excelência operacional por meio da aplicação confiável e eficiente da tecnologia.
- Manter o risco de TI em um nível aceitável.
- Otimizar o custo da tecnologia e dos serviços de TI.
- Cumprir as leis, regulamentos, acordos contratuais e políticas pertinentes cada vez mais presentes.

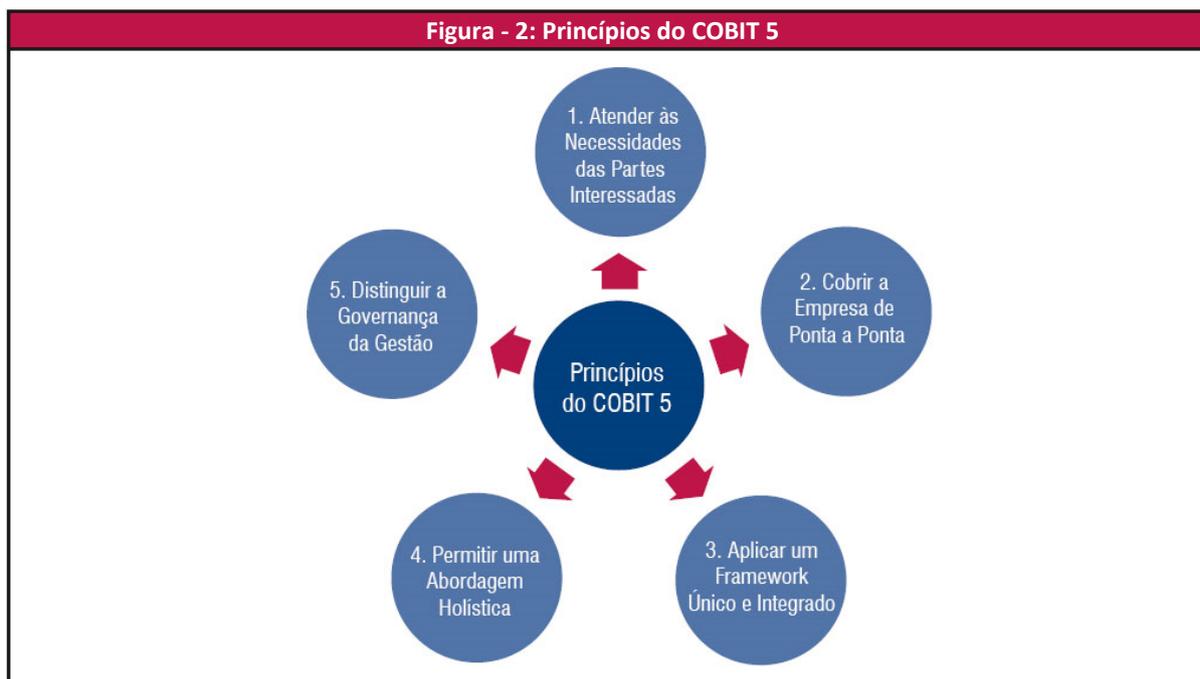
Durante a última década, o termo 'governança' ganhou um lugar de destaque no pensamento das organizações em resposta aos exemplos que demonstram a importância da boa governança e, do outro lado da balança, aos desafios dos negócios globais.

Organizações bem-sucedidas reconhecem que a diretoria e os executivos devem aceitar que a TI é tão significativa para os negócios como qualquer outra parte da organização. Diretores e gestores - seja em funções de TI ou de negócios - devem colaborar e trabalhar em conjunto a fim de garantir que a TI esteja inclusa na abordagem de governança e gestão. Além disso, cada vez mais leis e regulamentos estão sendo aprovados e estabelecidos para atender a essa necessidade.

O COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI. Em termos simples, O COBIT 5 ajuda as organizações a criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos. O COBIT 5 permite que a TI seja governada e gerida de forma holística para toda a organização, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI. O COBIT 5 é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.

Figura - 2: Princípios do COBIT 5

1. Atender às Necessidades das Partes Interessadas
2. Cobrir a Empresa de Ponta a Ponta
3. Aplicar um Framework Único e Integrado
4. Permitir uma Abordagem Holística
5. Distinguir a Governança da Gestão

Princípios do COBIT 5

O COBIT 5 baseia-se em cinco princípios básicos (demonstrados na figura 2) para governança e gestão de TI da organização:

- **1º Princípio: Atender às Necessidades das Partes Interessadas** - Organizações existem para criar valor para suas Partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. O COBIT 5 fornece todos os processos necessários e demais habilitadores para apoiar a criação de valor para a organização com o uso de TI. Como cada organização tem objetivos diferentes, o COBIT 5 pode ser personalizado de forma a adequá-lo ao seu próprio contexto por meio da cascata de objetivos, ou seja, traduzindo os objetivos corporativos em alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos.
- **2º Princípio: Cobrir a Organização de Ponta a Ponta** - O COBIT 5 integra a governança corporativa de TI organização à governança corporativa:

- Cobre todas as funções e processos corporativos; O COBIT 5 não se concentra somente na 'função de TI', mas considera a tecnologia da informação e tecnologias relacionadas como ativos que devem ser tratados como qualquer outro ativo por todos na organização.
- Considera todos os habilitadores de governança e gestão de TI aplicáveis em toda a organização, de ponta a ponta, ou seja, incluindo tudo e todos - interna e externamente - que forem considerados relevantes para a governança e gestão das informações e de TI da organização.

- **3º Princípio: Aplicar um Modelo Único Integrado** - Há muitas normas e boas práticas relacionadas a TI, cada qual provê orientações para um conjunto específico de atividades de TI. O COBIT 5 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como o um modelo unificado para a governança e gestão de TI da organização.
- **4º Princípio: Permitir uma Abordagem Holística** - Governança e gestão eficiente e eficaz de TI da organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização. Habilitadores são geralmente definidos como qualquer coisa que possa ajudar a atingir os objetivos corporativos. O modelo do COBIT 5 define sete categorias de habilitadores:
  - Princípios, Políticas e Modelos
  - Processos
  - Estruturas Organizacionais
  - Cultura, Ética e Comportamento
  - Informação
  - Serviços, Infraestrutura e Aplicativos
  - Pessoas, Habilidades e Competências
- **5º Princípio: Distinguir a Governança da Gestão** – O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciadas e servem a propósitos diferentes. A visão do COBIT 5 sobre esta importante distinção entre governança e gestão é:

  - Governança

A governança garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.

Na maioria das organizações, a governança geral é de responsabilidade do conselho de administração sob a liderança do presidente. Responsabilidades de governança específicas podem ser delegadas a modelos organizacionais especiais no nível adequado, especialmente em organizações complexas de grande porte.

  - Gestão

A gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.

Na maioria das organizações, a gestão é de responsabilidade da diretoria executiva sob a liderança do diretor executivo (CEO).

Juntos, esses cinco princípios permitem que a organização crie um modelo eficiente de governança e gestão otimizando os investimentos em tecnologia da informação e seu uso para o benefício das partes interessadas.

CAPÍTULO 1
VISÃO GERAL DO COBIT 5

O COBIT 5 fornece a próxima geração de orientações da ISACA sobre governança corporativa e gestão de TI. Baseia-se em mais de 15 anos de uso e aplicação prática do COBIT por muitas organizações e usuários das comunidades de negócios, TI, risco, segurança e garantia. Os principais fatores para o desenvolvimento do COBIT 5 incluem as necessidades de:

- Permitir que mais partes interessadas falem sobre o que eles esperam da tecnologia da informação e tecnologias relacionadas (que benefícios e em qual nível de risco aceitável e a qual custo) e quais são suas prioridades para garantir que o valor esperado seja efetivamente obtido. Alguns vão querer retornos no curto prazo e outros irão preferir a sustentabilidade no longo prazo. Alguns estarão preparados para assumir um alto risco enquanto outros não. Essas expectativas divergentes e por vezes conflitantes precisam ser tratadas com eficiência. Além disso, estas partes interessadas não só desejam estar mais envolvidos, como também querem mais transparência em relação a como isso irá acontecer e aos resultados reais obtidos.
- Abordar a questão da dependência cada vez maior para o sucesso da organização em parceiros externos de TI e de negócios tais como terceirizadas, fornecedores, consultores, clientes, provedores de serviços na nuvem e demais serviços, e de um conjunto diversificado de meios e mecanismos internos para entregar do valor esperado.
- Tratar a quantidade de informação, que tem aumentado significativamente. Como as organizações selecionam a informação relevante e confiável que levará a decisões de negócios corretas e eficientes? A informação também precisa ser gerenciada de forma eficaz e um modelo eficiente para o tratamento da informação pode ajudar.
- Administrar TI cada vez mais pervasiva; TI é cada vez mais uma parte integrante do negócio. Muitas vezes, já não basta manter a TI separada mesmo que esteja alinhada ao negócio. Ela precisa ser uma parte integrante dos projetos organizacionais, estruturas organizacionais, gestão de risco, políticas, capacidades, processos, etc. As funções do diretor de TI (CIO) e da área de TI estão evoluindo. Cada vez mais executivos de negócios têm habilidades em TI e estão, ou estarão, envolvidos em decisões de TI e operações de TI. Negócio e TI terão de ser mais bem integradas.
- Fornecer mais orientações na área de tecnologias emergentes e inovadoras; isto tem a ver com criatividade, inventividade, desenvolvimento de novos produtos, tornar os produtos atuais mais interessantes para os clientes e conquistar novos tipos de clientes. Inovação também pressupõe a dinamização do desenvolvimento do produto, dos processos de produção e da cadeia de suprimentos visando fornecer produtos ao mercado com níveis mais altos de eficiência, rapidez e qualidade.
- Cobrir o negócio de ponta a ponta e todas as áreas responsáveis pelas funções de TI, bem como todos os aspectos que levam à eficiente governança e gestão de TI da organização, tais como estruturas organizacionais, políticas e cultura, ao longo e acima dos processos.
- Obter melhor controle sobre o crescente número de soluções de TI que são de iniciativa dos usuários e estão sendo gerenciadas por eles.
- Atingir:
  - Criação de valor para a organização através do uso eficiente e inovador de TI da organização
  - Satisfação dos usuários de negócio com os serviços de TI
  - Cumprimento das leis, regulamentos, acordos contratuais e políticas internas pertinentes
  - Uma melhoria das relações entre as necessidades corporativas e os objetivos de TI
- Conectar-se e, quando pertinente, alinhar-se a outros importantes padrões e modelos do mercado, tais como: *Information Technology Infrastructure Library* (ITIL®), *The Open Group Architecture Framework* (TOGAF®), *Project Management Body of Knowledge* (PMBOK®), *PRojects IN Controlled Environments 2* (PRINCE2®), *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) e *International Organization for Standardization* (ISO). Isto ajudará as Partes Interessadas a entender como os diversos modelos, boas práticas e padrões se inter-relacionam e como elas podem ser usadas em conjunto.
- Integrar todas os principais modelos e orientações da ISACA, com o foco principal no COBIT, Val IT e Risk IT, mas considerando também o Modelo de Negócios para Segurança da Informação (BMIS), o Modelo de Garantia de TI (ITAF), a publicação intitulada *Board Briefing on IT Governance*, e o recurso *Taking Governance Forward* (TGF), de tal forma que o COBIT 5 cubra toda a organização e forneça uma base para integrar estes outros modelos outros modelos, padrões e práticas como um modelo único.

Outros produtos e orientações que cobrem as diferentes necessidades das diversas partes interessadas serão criados a partir da base de conhecimento principal do COBIT 5. Isto acontecerá com o tempo, tornando a arquitetura do produto COBIT 5 um documento vivo. A arquitetura mais recente do produto COBIT 5 pode ser encontrada nas páginas do COBIT no website da ISACA (*www.isaca.org/cobit*).

Visão Geral desta Publicação

O modelo do COBIT 5 contém mais sete capítulos:

- O Capítulo 2 trata do 1º Princípio, **Atender às necessidades das Partes interessadas**. Ele apresenta a cascata dos objetivos do COBIT 5. Os objetivos corporativos de TI são usados para formalizar e estruturar as necessidades das partes interessadas. Os objetivos corporativos podem estar associados aos objetivos de TI, e esses objetivos de TI podem ser alcançados através do uso e execução otimizados de todos os habilitadores, inclusive processos. Este conjunto de objetivos interligados é chamado de cascata dos objetivos do COBIT 5. O capítulo também inclui exemplos de perguntas típicas sobre governança e gestão que os Partes Interessadas poderão fazer sobre a TI da organização.
- O Capítulo 3 trata do 2º Princípio, **Cobrir a organização de ponta a ponta**. Este capítulo explica como o COBIT 5 integra a governança corporativa de TI à governança corporativa empresarial cobrindo todas as funções e processos da organização.
- O Capítulo 4 trata do 3º Princípio, **Aplicar um modelo Único Integrado**, e descreve brevemente a arquitetura do COBIT 5 que atinge a integração.
- O Capítulo 5 trata do 4º Princípio, **Permitir uma Abordagem Holística**. A governança corporativa de TI é sistêmica e apoiada por um conjunto de habilitadores. Neste capítulo, os habilitadores são apresentados juntamente com uma maneira comum de se olhar para eles: o modelo do habilitador genérico.
- O Capítulo 6 trata do 5º Princípio, **Distinguir a Governança da Gestão**, e discute a diferença entre gestão e governança, e como elas se inter-relacionam. O modelo de referência do processo de alto nível do COBIT 5 é incluído como exemplo.
- O Capítulo 7 contém uma introdução ao **Guia de Implementação**. Ele descreve como o ambiente adequado pode ser criado, os habilitadores necessários, pontos fracos comuns e problemas típicos da implementação, bem como a implementação e melhoria contínua do ciclo de vida. Este capítulo baseia-se na publicação intitulada **COBIT® 5 Implementação**, onde podem ser encontrados todos os detalhes sobre como implementar a governança corporativa de TI com base no COBIT 5.
- O Capítulo 8 trata do **Modelo de Capacidade de Processo do COBIT 5** contido no esquema da abordagem ao Programa de Avaliação do COBIT (*www.isaca.org/cobit-assessment-programme*), como ele difere das avaliações de maturidade de processo do COBIT 4.1, e como os usuários podem migrar para a nova abordagem.

Os apêndices contêm referências, mapeamentos e informações mais detalhadas sobre temas específicos:

- Apêndice A. **Referências** usadas durante o desenvolvimento do COBIT 5 são relacionadas aqui.
- Apêndice B. **Mapeamento Detalhado dos Objetivos Corporativos - Objetivos de TI** descreve como os objetivos corporativos são geralmente apoiados por um ou mais objetivos de TI.
- Apêndice C. **Mapeamento Detalhado dos Objetivos de TI - Processos de TI** descreve como os processos do COBIT apoiam o atingimento dos objetivos de TI.
- Apêndice D. **Necessidades das Partes Interessadas e Objetivos Corporativos** descreve como as necessidades básicas das Partes Interessadas partes interessadas se relacionam com os objetivos corporativos do COBIT 5.
- Apêndice E. Mapeamento do COBIT 5 Com os Padrões e Modelos Correlatos Mais Relevantes
- Apêndice F. Comparação entre o Modelo de Informações do COBIT 5 e os Critérios de Informações do COBIT 4.1.
- Apêndice G. **Descrição Detalhada dos Habilitadores do COBIT 5** baseia-se no capítulo 5 e inclui mais detalhes sobre os diferentes habilitadores, inclusive um modelo do habilitador detalhado com a descrição de componentes específicos e ilustrado com diversos exemplos.
- Apêndice H. **Glossário**

CAPÍTULO 2
1º PRINCÍPIO: ATENDER ÀS NECESSIDADES DAS PARTES INTERESSADAS

Introdução

As organizações existem para criar valor para suas partes interessadas. Consequentemente, qualquer organização — comercial ou não — terá a criação de valor como um objetivo da governança. Criar valor significa realizar benefícios com uma ótima relação de custo e ainda otimizar o risco (ver figura 3). Os benefícios podem assumir muitas formas, por exemplo, financeiros para organizações comerciais ou de serviço público para entidades governamentais.

Figura - 3: Objetivo da Governança: Criação de Valor

Necessidades das Partes Interessadas
Direcionam
Objetivo da Governança: Criação de Valor
Realização de Benefícios
Otimização do Risco
Otimização dos Recursos

As organizações têm muitas partes interessadas e ‘criar valor’ pode significar coisas diferentes - e por vezes conflitantes - para cada um deles. Governança tem a ver com negociar e decidir entre os interesses de valor das diferentes partes interessadas. Por consequência, o sistema de governança deve considerar todas as todas as partes interessadas ao tomar decisões sobre a avaliação dos recursos, benefícios e riscos. Para cada decisão, as seguintes perguntas podem e devem ser feitas: Para quem são os benefícios? Quem assume o risco? Que recursos são necessários?

Cascata dos Objetivos do COBIT 5

Cada organização opera em um contexto diferente; este contexto é determinado por fatores externos (mercado, setor, geopolíticas, etc.) e fatores internos (cultura, organização, inclinação ao risco, etc.), e exige um sistema de governança e gestão personalizado.

As necessidades das partes interessadas devem ser transformadas em uma estratégia exequível pela organização. A cascata de objetivos da organização. A cascata de objetivos do COBIT 5 é o mecanismo de tradução das necessidades das partes interessadas em objetivos corporativos específicos, personalizados, exequíveis, objetivos de TI e metas de habilitador. Esta tradução permite a configuração de objetivos específicos em cada nível e em cada área da organização em apoio aos objetivos gerais e às exigências das partes interessadas e, portanto, apoia efetivamente o alinhamento entre as necessidades corporativas e os serviços e soluções de TI.

A cascata de objetivos do COBIT 5 é demonstrado na figura 4.

1º Passo. Os Direcionadores das Partes Interessadas Influenciam as Necessidades das Partes Interessadas

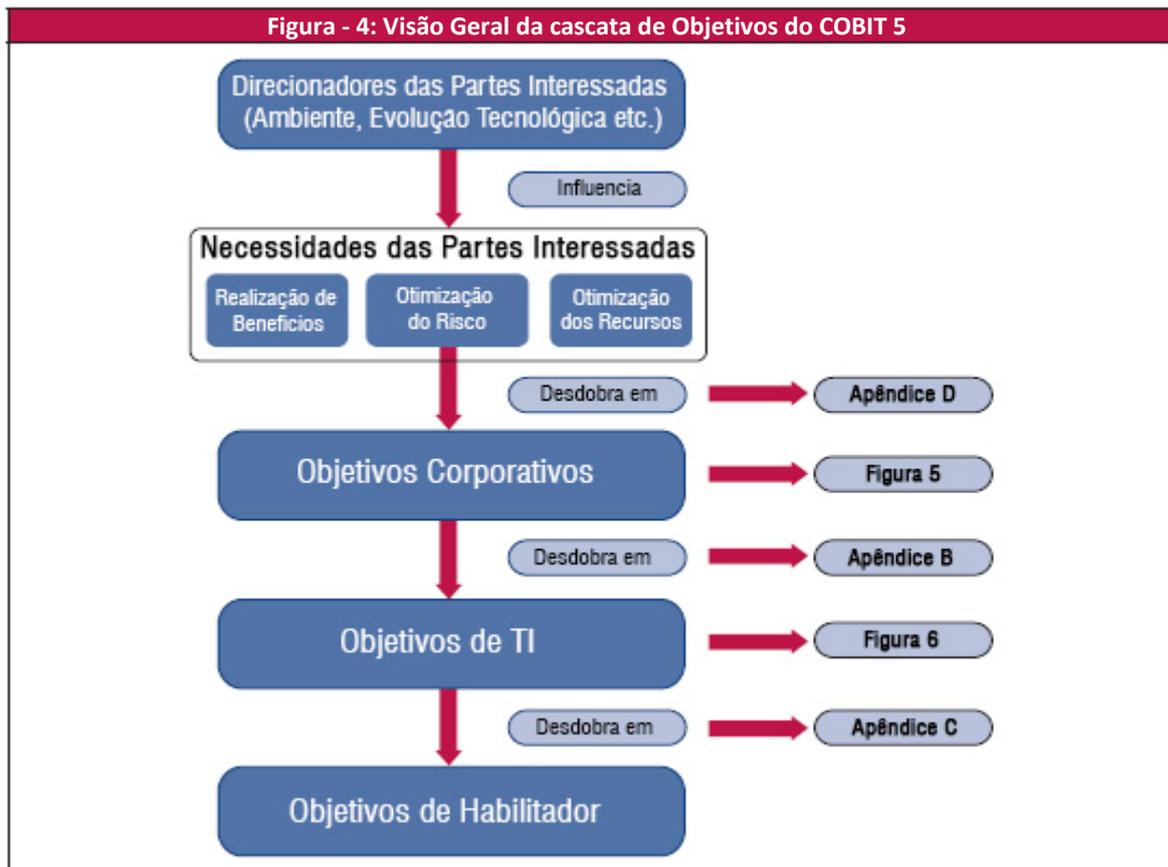
As necessidades das partes interessadas são influenciadas por diversas tendências, por exemplo, mudanças de estratégia, mudanças nos negócios e no ambiente regulatório bem como novas tecnologias.

2º Passo. Desdobramento das Necessidades das Partes Interessadas em Objetivos Corporativos

As necessidades das partes interessadas podem estar relacionadas a um conjunto de objetivos corporativos genéricos. Esses objetivos corporativos foram criados usando as dimensões do *balanced scorecard* (BSC)[1] e representam uma lista dos objetivos mais usados que uma organização pode definir para si. Embora esta lista não seja completa, a maioria dos objetivos específicos das organizações pode ser mapeada facilmente em um ou mais dos objetivos corporativos genéricos. Uma tabela com as necessidades das partes interessadas e os objetivos corporativos é apresentada no Apêndice D.

[1] Kaplan, Robert S.; David P. Norton; The Balanced Scorecard: Translating Strategy Into Action, Harvard University Press, EUA, 1996.

Figura - 4: Visão Geral da cascata de Objetivos do COBIT 5

Direcionadores das Partes Interessadas (Ambiente, Evolução Tecnológica etc.)
Influencia
Necessidades das Partes Interessadas
Realização de Benefícios
Otimização do Risco
Otimização dos Recursos
Desdobra em
Apêndice D
Objetivos Corporativos
Figura 5
Desdobra em
Apêndice B
Objetivos de TI
Figura 6
Desdobra em
Apêndice C
Objetivos de Habilitador

O COBIT 5 define 17 objetivos genéricos, conforme demonstrados na figura 5, que incluem as seguintes informações:

- A dimensão BSC sob a qual o objetivo corporativo se enquadra
- Objetivos corporativos
- A relação entre os três principais objetivos da governança – Realização de benefícios, Otimização do risco e Otimização dos recursos ('P' significa relação primária e 'S' relação secundária, ou seja, uma relação mais fraca).

3º Passo. Cascata dos Objetivos Corporativos em Objetivos de TI

O atingimento dos objetivos corporativos exige uma série de resultados de TI[2] que são representados pelos objetivos relacionados a TI. "Relacionados a TI" significa tudo o que estiver relacionado à tecnologia da informação e tecnologias afins, e os objetivos de TI são estruturados de acordo com as dimensões do *balanced scorecard* de TI (IT BSC). O COBIT 5 define 17 objetivos de TI, relacionados na **figura 6**.

A tabela de mapeamento dos objetivos corporativos em objetivos de TI foi incluída no Apêndice B, e demonstra como cada objetivo corporativo é apoiado por diversos objetivos de TI.

4º Passo. Cascata dos Objetivos de TI em Metas do Habilitador

Atingir os objetivos de TI exige a aplicação e o uso bem-sucedido de diversos habilitadores. O conceito de habilitador é explicado em detalhes no capítulo 5. Habilitadores incluem processos, estruturas organizacionais e informações, e para cada habilitador um conjunto específico de metas relevantes pode ser definido para apoiar os objetivos de TI.

Processos são um dos habilitadores, e o Apêndice C contém o mapeamento entre os objetivos de TI e os processos pertinentes do COBIT 5, que por sua vez contêm os respectivos objetivos do processo.

[2] Os resultados de TI não são obviamente o único benefício intermediário necessário para a consecução dos objetivos corporativos. Todas as demais áreas funcionais de uma organização, tais como finanças e marketing, também contribuem para a consecução dos objetivos corporativos, mas no contexto do COBIT 5 somente as atividades e os objetivos de TI são considerados

Figura - 5: Objetivos Corporativos do COBIT 5

Dimensão BSC	Objetivo corporativo	Relação com Objetivos de Governança		
		Realização de Benefícios	Otimização de Risco	Otimização de Recursos
Financeira	1. Valor dos investimentos da organização percebidos pelas partes interessadas	P		S
	2. Portfólio de produtos e serviços competitivos	P	P	S
	3. Gestão do risco do negócio (salvaguarda de ativos)		P	S
	4. Conformidade com as leis e regulamentos externos		P	
	5. Transparência financeira	P	S	S
Cliente	6. Cultura de serviço orientada ao cliente	P		S
	7. Continuidade e disponibilidade do serviço de negócio		P	
	8. Respostas rápidas para um ambiente de negócios em mudança	P		S
	9. Tomada de decisão estratégica com base na informação	P	P	P
	10. Otimização dos custos de prestação de serviços	P		P
Interna	11. Otimização da funcionalidade do processo de negócio	P		P
	12. Otimização dos custos do processo de negócio	P		P
	13. Gestão de programas de mudanças de negócios	P	P	S
	14. Produtividade operacional e da equipe	P		P
	15. Conformidade com as políticas internas		P	
Treinamento e Crescimento	16. Pessoas qualificadas e motivadas	S	P	P
	17. Cultura de inovação de produtos e negócios	P		

Figura - 6: Objetivos de TI

Dimensão BSC de TI	Objetivo da Informação e Tecnologia Relacionada	
Financeira	01	Alinhamento da estratégia de negócios e de TI
	02	Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos
	03	Compromisso da gerência executiva com a tomada de decisões de TI
	04	Gestão de risco organizacional de TI
	05	Benefícios obtidos pelo investimento de TI e portfólio de serviços
	06	Transparência dos custos, benefícios e riscos de TI
Cliente	07	Prestação de serviços de TI em consonância com os requisitos de negócio
	08	Uso adequado de aplicativos, informações e soluções tecnológicas
Interna	09	Agilidade de TI
	10	Segurança da informação, infraestrutura de processamento e aplicativos
	11	Otimização de ativos, recursos e capacidades de TI
	12	Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia
	13	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos
	14	Disponibilidade de informações úteis e confiáveis para a tomada de decisão
	15	Conformidade de TI com as políticas internas
Treinamento e Crescimento	16	Equipes de TI e de negócios motivadas e qualificadas
	17	Conhecimento, expertise e iniciativas para inovação dos negócios

Usando a Cascata de Objetivos do COBIT 5

Benefícios da Cascata de Objetivos do COBIT 5

A cascata de objetivos[3] é importante porque permite a definição das prioridades de implementação, melhoria e garantia da governança corporativa de TI com base nos objetivos (estratégicos) da organização e no respectivo risco. Na prática, a cascata de objetivos:

- Define as metas e objetivos tangíveis e relevantes em vários níveis de responsabilidade
- Filtra a base de conhecimento do COBIT 5, com base nos objetivos corporativos, para extrair a orientação pertinente para inclusão na implementação, melhoria ou garantia de projetos específicos
- Identifica e comunica claramente como (por vezes de forma muito operacional) os habilitadores são importantes para o atingimento dos objetivos corporativos

Usando a Cascata de Objetivos do COBIT 5 com Atenção

A cascata de objetivos - com suas tabelas de mapeamento entre os objetivos corporativos e os objetivos de TI e entre os objetivos de TI e os habilitadores do COBIT 5 (inclusive processos) - não contém a verdade universal, e os usuários não devem tentar usá-lo de uma forma puramente mecânica, mas sim como um orientador. Há várias razões para isso, entre as quais:

- Cada organização tem prioridades diferentes em seus objetivos, e essas prioridades podem mudar com o tempo.
- As tabelas de mapeamento não fazem distinção entre o porte da organização e/ou o setor em que ela está inserida. Elas representam uma espécie de denominador comum de como, no geral, os diferentes níveis de objetivos se inter-relacionam.
- Os indicadores usados no mapeamento consideram dois níveis de importância ou relevância, sugerindo a existência de 'discretos' níveis de relevância, considerando que, de fato, o mapeamento será parecido com uma constante com vários níveis de correspondência.

Usando a Cascata de Objetivos do COBIT 5 na Prática

A partir do aviso legal acima, fica evidente que o primeiro passo que uma organização sempre deverá dar ao utilizar a cascata de objetivos é personalizar o mapeamento, levando em consideração sua situação específica. Em outras palavras, cada organização deverá criar sua própria cascata de objetivos, compará-lo com o COBIT e depois refiná-la.

Por exemplo, a organização poderá desejar:

- Converter as prioridades estratégicas em um "peso" ou importância específica para cada um dos objetivos corporativos.
- Validar os mapeamentos da cascata de objetivos, levando em consideração seu ambiente e setor específicos, etc.

EXEMPLO 1 – CASCATA DE OBJETIVOS
Uma organização define para si uma série de objetivos estratégicos, dos quais a melhoria da satisfação do cliente é o mais importante. A partir dali, ela deseja saber o que precisa ser melhorado em todos os aspectos relativos a TI.
A organização decide que definir a satisfação do cliente como a principal prioridade é equivalente a elevar a prioridade dos seguintes objetivos corporativos (extraídos da figura 5):
6. Cultura de serviço orientada ao cliente
7. Continuidade e disponibilidade do serviço de negócio
8. Respostas rápidas para um ambiente de negócios em mudança
A organização dá agora o próximo passo na cascata dos objetivos: analisar quais objetivos de TI correspondem a esses objetivos corporativos. Uma sugestão de mapeamento entre eles foi relacionada no Apêndice B.
A partir dali, os seguintes objetivos de TI são sugeridos como os mais importantes (todos como relacionamentos 'P'):
01 Alinhamento da estratégia de TI e de negócios
04 Gestão do risco organizacional de TI
07 Prestação de serviços de TI em consonância com os requisitos de negócio
09 Agilidade de TI
10 Segurança da informação, infraestrutura de processamento e aplicativos
14 Disponibilidade de informações úteis e confiáveis para tomada de decisão
17 Conhecimento, expertise e iniciativas para inovação dos negócios
A organização valida esta lista e decide que os quatro primeiros objetivos serão considerados prioridade.
No próximo passo da cascata, usando o conceito de habilitador (ver capítulo 5), esses objetivos de TI levam a diversas metas de habilitador, que incluem objetivos do processo. No Apêndice C, um mapeamento é sugerido entre os objetivos de TI e os processos do COBIT 5. Aquela tabela permite a identificação dos mais importantes processos de TI que apoiam os objetivos de TI, porém, os processos por si só não são suficientes. Os demais habilitadores, tais como cultura, comportamento e ética; modelos organizacionais ou habilidades e expertise são igualmente importantes e requerem um conjunto de objetivos bem definidos.
Quando este exercício for concluído, a organização terá um conjunto de metas consistentes para todos os habilitadores que permitirão que ela alcance os objetivos estratégicos estabelecidos, além de um conjunto de indicadores correlatos para medir o desempenho

[3] A cascata de objetivos baseia-se na pesquisa realizada pelo Instituto de Governança e Alinhamento de TI da Faculdade de Administração da Universidade de Antuérpia, na Bélgica.

EXEMPLO 2 - NECESSIDADES DAS PARTES INTERESSADAS: SUSTENTABILIDADE
Após a conclusão da análise das necessidades das partes interessadas, a organização decide que a sustentabilidade é uma prioridade estratégica. Para ela, a sustentabilidade inclui não só os aspectos ambientais, mas todas as coisas que contribuem para o sucesso da organização no longo prazo.
Com base nos resultados da análise das necessidades das partes interessada, a organização decide concentrar-se nos cinco objetivos abaixo, com especificações mais detalhadas:
1. Valor dos investimentos da organização percebidos pelas partes interessada, especialmente pela sociedade das partes interessadas
4. Conformidade com as leis e regulamentos externos, com foco nas leis ambientais e leis trabalhistas que tratam dos contratos de terceirização
8. Resposta rápida para um ambiente de negócios em mudança
16. Pessoas qualificadas e motivadas, que reconhecem que o sucesso da organização depende de seus colaboradores
17. Cultura de inovação de produtos e negócios, com foco em inovações no longo prazo
Com base nessas prioridades, a cascata de objetivos pode ser aplicada conforme explicado no texto

Perguntas sobre Governança e Gestão de TI

O atendimento das necessidades das partes interessadas de qualquer organização - devido à elevada dependência de TI - levantará diversas perguntas sobre governança e gestão de TI da organização (figura 7).

Figura - 7: Perguntas sobre Governança e Gestão de TI	
Partes Interessadas Internas	**Perguntas das Partes Interessadas Internas**
• Conselho • Diretor Executivo (CEO) • Diretor Financeiro (CFO) • Diretor de Informática (CIO) • Diretor de Risco (CRO) • Executivos de Negócios • Proprietários de processos de negócio • Gerentes de negócios • Gerentes de risco • Gerentes de segurança • Gerentes de serviços • Gerentes de Recursos Humanos (RH) • Auditores internos • Diretores de privacidade • Usuários de TI • Gerentes de TI • Etc.	• Como faço para obter valor com o uso de TI? Os usuários finais estão satisfeitos com a qualidade do serviço de TI? • Como posso gerenciar o desempenho de TI? • Como posso explorar melhor as novas tecnologias para novas oportunidades estratégicas? • Como faço para criar e estruturar da melhor forma o meu departamento de TI? • Qual é a minha dependência de fornecedores externos? Quão bem os contratos de terceirização de TI estão sendo administrados? • Como faço para obter garantia dos fornecedores externos? • Quais são os requisitos (de controle) da informação? • Considerei todos os riscos de TI? • Estou conduzindo uma sólida e eficiente operação de TI? • Como posso controlar o custo de TI? Como utilizar os recursos de TI de forma mais eficaz e eficiente? • Quais são as opções de terceirização mais eficazes e eficientes? • Tenho pessoal suficiente para TI? Como faço para desenvolver e manter sua capacitação, e como controlo seu desempenho? • Como faço para obter garantia de TI? • As informações que estou processando estão bem protegidas? • Como posso melhorar a agilidade dos negócios com um ambiente de TI mais flexível? • Os projetos de TI não cumprem o que prometeram – e caso afirmativo, por quê? TI está atrapalhando a execução da estratégia de negócios? • Quão crítica é TI para a sustentação da organização? O que fazer se ela não estiver disponível? • Quais processos de negócios críticos dependem de TI, e quais são os requisitos dos processos de negócios? • Qual tem sido o custo adicional médio dos orçamentos operacionais de TI? Com que frequência e em que medida os projetos de TI estouram o orçamento? • Quanto do esforço de TI é dedicado para apagar incêndios em vez de facilitar a melhoria do negócio? • Foram disponibilizados infraestruturas e recursos de TI suficientes para alcançar os objetivos estratégicos da organização? • Quanto tempo é necessário para a tomada de decisões importantes de TI? • O esforço total de TI e seus investimentos são transparentes? • TI apoia a organização no cumprimento dos regulamentos e níveis de serviço? Como faço para saber se estou em conformidade com todos os regulamentos aplicáveis?
Partes Interessadas Externas	**Perguntas das Partes Interessadas Externas**
• Parceiros comerciais • Fornecedores • Acionistas • Reguladores/governo • Usuários externos • Clientes • Organizações de normatização • Auditores externos • Consultores • Etc.	• Como posso saber se as operações do meu parceiro comercial são seguras e confiáveis? • Como posso saber se a organização cumpre as regras e regulamentos aplicáveis? • Como posso saber se a organização mantém um sistema eficiente de controle interno? • Os parceiros comerciais têm a cadeia de informações entre eles sob controle?

Como Encontrar uma Resposta para Essas Perguntas

Todas as perguntas mencionadas na figura 7 podem estar relacionadas aos objetivos corporativos, e servem como entrada para a cascata de objetivos, sobre os quais podem ser abordados com eficiência. O Apêndice D contém um exemplo de mapeamento entre as perguntas das partes interessadas internas mencionadas na **figura 7** e os objetivos corporativos.

CAPÍTULO 3
2º PRINCÍPIO: COBRIR A ORGANIZAÇÃO DE PONTA A PONTA

O COBIT 5 aborda a governança e gestão da informação e da tecnologia correlata a partir da perspectiva de toda a organização, de ponta a ponta. Isso significa que o COBIT 5:

- Integra a governança corporativa de TI à governança corporativa da organização. Ou seja, o sistema de governança corporativa de TI proposto pelo COBIT 5 integra-se perfeitamente em qualquer sistema de governança. O COBIT 5 alinha-se com as últimas visões sobre governança.
- Cobre todas as funções e processos necessários para regular e controlar as informações da organização e tecnologias correlatas onde quer que essas informações possam ser processadas. Considerando este amplo escopo organizacional, o COBIT 5 trata de todos os serviços de TI internos e externos pertinentes, bem como dos processos de negócios internos e externos.

O COBIT 5 fornece uma visão holística e sistêmica sobre a governança e gestão de TI da organização (ver princípio 4), que tem por base diversos habilitadores. Os habilitadores servem para toda a organização, de ponta a ponta, ou seja, incluem todas as pessoas e todas as coisas, internas e externas, pertinentes à governança e gestão das informações e TI da organização, inclusive as atividades e responsabilidades das funções corporativas de TI bem como aquelas não relacionadas com essas funções.

Informação é uma das categorias de habilitadores do COBIT. O modelo pelo qual o COBIT 5 define os habilitadores permite que cada parte interessada defina requisitos abrangentes e completos para as informações e para o ciclo de vida de processamento das informações, associando assim o negócio e suas necessidades de informações adequadas à função de TI, e apoiando a organização e o foco no contexto.

Abordagem à Governança

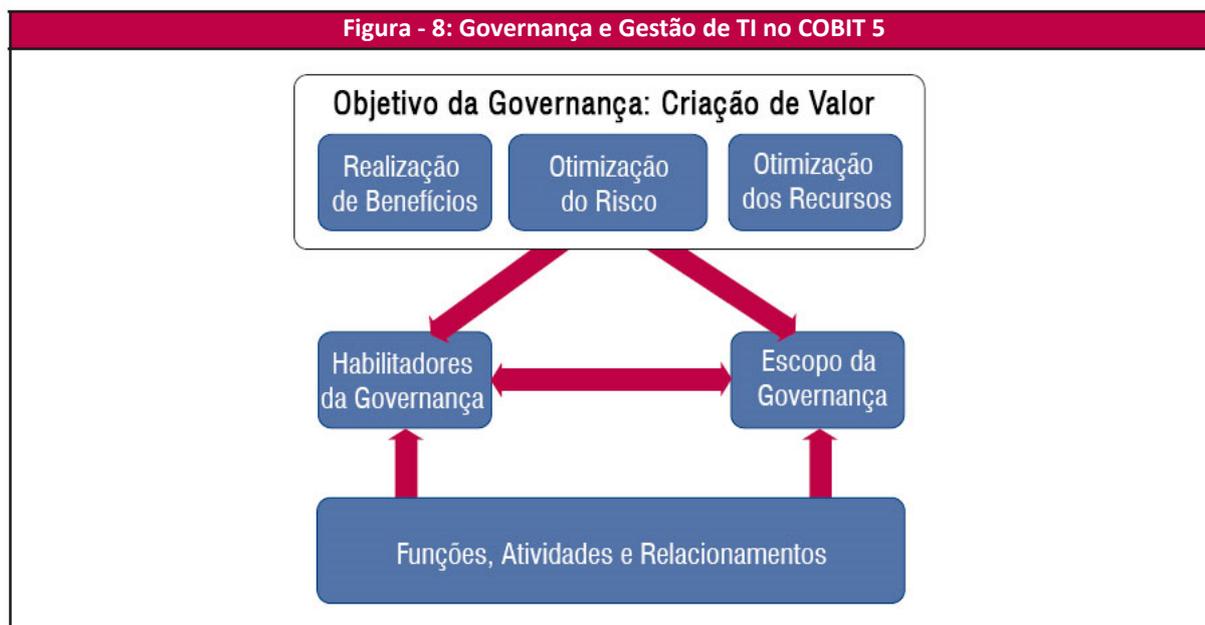
A abordagem à governança de ponta a ponta que está na base do COBIT 5 é demonstrada na figura 8, onde podem ser observados os principais componentes de um sistema de governança.[4]

Figura - 8: Governança e Gestão de TI no COBIT 5

Objetivo da Governança: Criação de Valor

Realização de Benefícios | Otimização do Risco | Otimização dos Recursos

Habilitadores da Governança ↔ Escopo da Governança

Funções, Atividades e Relacionamentos

[4] Este sistema de governança é uma ilustração da iniciativa *Taking Governance Forward* (TGF) da ISACA; para mais informações sobre o TGF acesse: *www.takinggovernanceforward.org*.

Além do objetivo de governança, os outros principais elementos da abordagem à governança incluem habilitadores; escopo; além de funções, atividades e relacionamentos.

Habilitadores da Governança

Habilitadores da governança são os recursos organizacionais da governança, tais como modelos, princípios, processos e práticas, por meio dos quais a ação é orientada e os objetivos podem ser alcançados. Os habilitadores também incluem os recursos da organização - por exemplo, capacidades do serviço (infraestrutura de TI, aplicativos, etc.), pessoas e informações. A falta de recursos ou habilitadores poderá afetar a capacidade da organização na criação de valor.

Devido a importância dos habilitadores da governança, o COBIT 5 inclui uma forma única de olhar e lidar com esses habilitadores (ver capítulo 5).

Escopo da Governança

A governança pode ser aplicada a toda a organização, uma entidade, um ativo tangível ou intangível, etc. Ou seja, podem-se definir diferentes visões da organização às quais a governança será aplicada, e é fundamental definir bem este escopo do sistema de governança. O escopo do COBIT 5 é a organização - mas, em suma, o COBIT 5 pode tratar de qualquer dessas diferentes visões.

Papéis, Atividades e Relacionamentos

Um último elemento refere-se às papéis, atividades e relacionamentos de governança. Ele define quem está envolvido na governança, como estão envolvidos, o que fazem e como interagem, dentro do escopo de qualquer sistema de governança. O COBIT 5 faz uma clara diferenciação entre as atividades de governança e gestão nos domínios de governança e gestão, bem como a interação entre elas e os especialistas envolvidos. A **figura 9** mostra em detalhes a parte inferior da figura 8, com as interações entre os diferentes papéis.

Para mais informações sobre esta visão de governança genérica, ver a iniciativa "*Taking Governance Forward*" em: www.takinggovernanceforward.org.

Figura - 9: Principais Funções, Atividades e Relacionamentos

Funções, Atividades e Relacionamentos

Proprietários e Partes Interessadas
Delegam
Responsabiliza
Conselho de Administração
Define Orientação
Monitora
Corpo Diretivo
Instrui e Alinha
Reportam
Operações e Execução

CAPÍTULO 4
3º PRINCÍPIO: APLICAR UM MODELO ÚNICO INTEGRADO

O COBIT 5 é um modelo único e integrado porque:

- Alinha-se com outros padrões e modelos mais recentes, permitindo assim que a organização use o COBIT 5 como o principal integrador do modelo de governança e gestão.
- É completo na cobertura da organização, fornecendo a base para integrar com eficiência outros modelos, padrões e práticas utilizados. Um modelo único principal serve como uma fonte consistente e integrada de orientação em uma linguagem comum, não técnica, agnóstico-tecnológica.
- Fornece uma arquitetura simples para estruturação dos materiais de orientação e produção de um conjunto consistente de produtos.
- Integra todo o conhecimento previamente disperso nos diversos modelos da ISACA. A ISACA vem pesquisando a principal área de governança corporativa há muitos anos e criou modelos tais como COBIT, Val IT, Risk IT, BMIS, a publicação *Board Briefing on IT Governance*, e ITAF para prestar orientação e assistência às organizações.

O COBIT 5 integra todo este conhecimento.

Integrador de Modelos do COBIT 5

A figura 10 apresenta uma descrição gráfica de como o COBIT 5 cumpre seu papel de modelo alinhado e integrado

Figura - 10: Modelo Único Integrado do COBIT 5

Orientação ISACA (COBIT, Val IT, Risk IT, BMIS, ...)
Novos Materiais de Orientação da ISACA
Outros Padrões e Frameworks
Base de Conhecimento do COBIT 5
• Orientação e conteúdo atuais
• Estrutura para conteúdos futuros
Habilitadores do COBIT 5
Filtro de Conteúdo para a Base de Conhecimento
Família de Produtos COBIT 5
COBIT 5
Guias de Habilitadores do COBIT
Guias Profissionais do COBIT 5
Ambiente Colaborativo On-line do COBIT 5

O modelo do COBIT 5 oferece às partes interessadas a mais completa e atualizada orientação (ver figura 11) sobre governança e gestão de TI da organização através de:

- Pesquisa e utilização de um conjunto de fontes que têm impulsionado o desenvolvimento de conteúdo novo, inclusive:
  - Reunindo a orientação da ISACA existente (COBIT 4.1, Val IT 2.0, Risk IT e BMIS) neste modelo único
  - Complementando este conteúdo com áreas que necessitam de mais elaborações e atualizações
  - Alinhando-se com outros padrões e modelos relevantes, tais como os padrões ITIL, TOGAF e ISO. A lista completa de referências pode ser encontrada no Apêndice A
- Definição de um conjunto de habilitadores da governança e gestão, que fornece o modelo para todos os materiais de orientação
- Preenchimento da base de conhecimento do COBIT 5 que contém toda a orientação e o conteúdo já produzidos, assim como a disponibilização do modelo para novos conteúdos no futuro
- Fornecimento de uma base sólida e abrangente de referência de boas práticas

Figura - 11: Família de Produtos COBIT 5

COBIT® 5

Guias de Habilitadores do COBIT 5

COBIT® 5: Habilitador Processos

COBIT® 5: Habilitador Informação

Outros Guias de Habilitadores

Guias Profissionais do COBIT 5

COBIT® 5 Implementação

COBIT® 5 para Segurança da Informação

COBIT® 5 para Garantia (Assurance)

COBIT® 5 para Risco

Outros Guias Profissionais

Ambiente Colaborativo Online do COBIT® 5

CAPÍTULO 5
4º PRINCÍPIO: PERMITIR UMA ABORDAGEM HOLÍSTICA

Habilitadores do COBIT 5

Habilitadores são fatores que, individualmente e em conjunto, influenciam se algo irá funcionar - neste caso, a governança e a gestão corporativas da TI. Os habilitadores são orientados pela cascata de objetivos, ou seja, objetivos de TI em níveis mais alto definem o que os diferentes habilitadores deverão alcançar.

O modelo do COBIT 5 descreve sete categorias de habilitadores (figura 12):

- **Princípios, políticas e modelos** são veículos para a tradução do comportamento desejado em orientações práticas para a gestão diária.
- **Processos** descrevem um conjunto organizado de práticas e atividades para o atingimento de determinados objetivos e produzem um conjunto de resultados em apoio ao atingimento geral dos objetivos de TI.
- **Estruturas organizacionais** são as principais entidades de tomada de decisão de uma organização.
- **Cultura**, **ética e comportamento** das pessoas e da organização são muitas vezes subestimados como um fator de sucesso nas atividades de governança e gestão.
- **Informação** permeia qualquer organização e inclui todas as informações produzidas e usadas pela organização. A Informação é necessária para manter a organização em funcionamento e bem governada, mas no nível operacional, a informação por si só é muitas vezes o principal produto da organização.
- **Serviços, infraestrutura e aplicativos** incluem a infraestrutura, a tecnologia e os aplicativos que fornecem à organização o processamento e os serviços de tecnologia da informação.
- **Pessoas, habilidades e competências** estão associadas às pessoas e são necessárias para a conclusão bem-sucedida de todas as atividades bem como para a tomada de decisões corretas e tomada de medidas corretivas.

Figura - 12: Habilitadores Corporativos do COBIT 5

2. Processos
3. Estruturas Organizacionais
4. Cultura, Ética e Comportamento
1. Princípios, Políticas e Frameworks
5. Informação
6. Serviços, Infraestrutura e Aplicativos
7. Pessoas, Habilidades e Competências
Recursos

Alguns dos habilitadores definidos acima também são recursos da organização que devem ser gerenciados e governados. Isto se aplica:

- A Informação, que deve ser gerenciada como um recurso. Algumas informações, tais como relatórios de gestão e informações de inteligência organizacional são importantes habilitadores para a governança e gestão da organização.
- Serviços, infraestrutura e aplicativos.
- Pessoas, habilidades e competências.

Governança e Gestão Sistêmicas por meio de Habilitadores Interligados

A figura 12 também transmite uma ideia que deve ser adotada pela governança corporativa, incluindo a governança de TI, que é de atingir os principais objetivos corporativos. Uma organização sempre deverá considerar um conjunto de habilitadores interligados. Ou seja, cada habilitador:

- Necessita das informações dos demais habilitadores para ser plenamente efetivo, por exemplo, processos precisam de informações e modelos organizacionais necessitam de habilidades e comportamento.
- Produz resultados para o benefício dos demais habilitadores, por exemplo, os processos geram informações, e as habilidades e o comportamento tornam os processos eficientes.

Assim, ao tratar da governança e gestão corporativa de TI, boas decisões podem ser tomadas somente quando esta natureza sistêmica dos arranjos de governança e gestão for considerada. Isto significa que para tratar de qualquer necessidade das partes interessadas, a referência de todos os habilitadores inter-relacionados deve ser analisada e tratada, se necessário. Esta mentalidade deve ser orientada pela alta administração da organização, conforme ilustrado nos exemplos abaixo.

EXEMPLO 3 – GOVERNANÇA E GESTÃO CORPORATIVA DE TI DA ORGANIZAÇÃO
Prestar serviços operacionais de TI a todos os usuários exige capacidades de serviço (infraestrutura, aplicativos) bem como pessoas qualificadas e com o comportamento necessário. Diversos processos de prestação de serviços também devem ser implementados, apoiados pelas estruturas organizacionais adequadas, que demonstram como todos os habilitadores são necessários para uma prestação de serviços bem-sucedida.

EXEMPLO 4 - GOVERNANÇA E GESTÃO CORPORATIVA DE TI DA ORGANIZAÇÃO
A necessidade de segurança da informação exige a criação e adoção de diversas políticas e procedimentos. Essas políticas, por sua vez, exigem a implementação de diversas práticas de segurança. No entanto, se a cultura e a ética da organização e das pessoas não forem apropriadas, os processos e os procedimentos de segurança das informações não serão efetivos.

Dimensões dos Habilitadores do COBIT 5

Todos os habilitadores possuem um conjunto de dimensões comuns. Este conjunto de dimensões comuns (figura 13):

- Apresenta uma maneira comum, simples e estruturada para tratar dos habilitadores
- Permite que uma entidade controle suas interações complexas
- Facilita resultados bem-sucedidos dos habilitadores

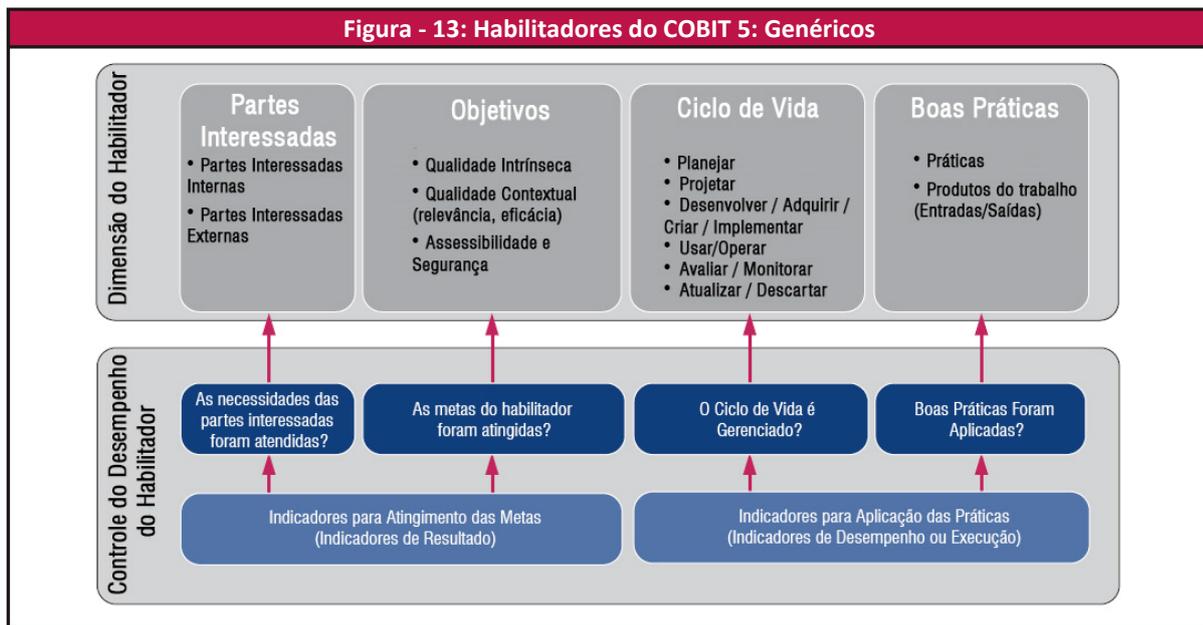



Figura - 13: Habilitadores do COBIT 5: Genéricos

Dimensões do Habilitador

As quatro dimensões comuns dos habilitadores são:

- **Partes Interessadas** - Cada habilitador tem partes interessadas (partes que desempenham um papel ativo e/ou tenham algum interesse no habilitador). Por exemplo, os processos têm diversas partes que executam atividades do processo e/ou que tenham algum interesse nos resultados do processo; estruturas organizacionais têm partes interessadas, cada um com suas próprias funções e interesses que fazem parte das estruturas. Partes interessadas podem ser internas ou externas à organização, e todas possuem seus próprios, e às vezes conflitantes, interesses e necessidades. As necessidades das partes interessadas são traduzidas em objetivos corporativos, que por sua vez são traduzidas em objetivos corporativos para organização. Uma lista de partes interessadas é apresentada na figura 7.
- **Metas** - Cada habilitador tem diversas metas, e os habilitadores criam valor ao atingir essas metas. Metas podem ser definidas em termos de:
  - Resultados esperados do habilitador
  - Aplicativo ou operação do próprio operador

As metas do habilitador são a última etapa da cascata de objetivos do COBIT 5. Essas metas podem ser divididas ainda em diferentes categorias:

- **Qualidade intrínseca** - O quanto os habilitadores trabalham de forma precisa, objetiva e produzem resultados exatos, objetivos e confiáveis
- **Qualidade contextual** - O quanto os habilitadores e seus resultados cumprem sua meta levando-se em consideração o contexto em que operam. Por exemplo, os resultados devem ser pertinentes, completos, atuais, apropriados, consistentes, compreensíveis e fáceis de usar.
- **Acesso e segurança** - O quanto os habilitadores e seus resultados são acessíveis e seguros, tais como:
  - Os habilitadores estão disponíveis quando, e se, necessário.
  - Os resultados são seguros, ou seja, o acesso é restrito a quem de direito e que precisar deles.

- **Ciclo de vida** - Cada habilitador tem um ciclo de vida, desde sua criação, passando por sua vida útil/operacional até chegar ao descarte. Isto se aplica às informações, estruturas, processos, políticas, etc. As fases do ciclo de vida incluem:
  - Planejar (inclui o desenvolvimento e seleção de conceitos)
  - Projetar
  - Desenvolver/adquirir/criar/implementar
  - Usar/operar
  - Avaliar/monitorar
  - Atualizar/descartar
- **Boas práticas** - Boas práticas podem ser definidas para cada um dos habilitadores. Boas práticas apoiam o atingimento das metas do habilitador. Boas práticas oferecem exemplos ou sugestões de como implementar o habilitador da melhor maneira, e quais produtos do trabalho ou entradas e saídas são necessários. O COBIT 5 oferece exemplos de boas práticas para alguns dos habilitadores do COBIT 5 (ex: processos). Para outros habilitadores pode-se usar a orientação dos demais padrões, modelos, etc.

Controle de Desempenho do Habilitador

Organizações esperam resultados positivos da aplicação e uso dos habilitadores. Para controlar o desempenho dos habilitadores, as perguntas abaixo terão de ser monitoradas e posteriormente respondidas - com base em Indicadores - periodicamente:

- As necessidades das partes interessadas foram consideradas?
- As metas do habilitador foram atingidas?
- O ciclo de vida do habilitador é controlado?
- Boas práticas foram aplicadas?

Os dois primeiros pontos tratam do resultado efetivo do habilitador. Os indicadores usados para aferir em que medida as metas foram atingidas podem ser chamadas de ‘indicadores de resultado’.

Os dois últimos pontos tratam do funcionamento efetivo do próprio habilitador, e estes indicadores podem ser chamadas de ‘indicadores de progresso’.

Exemplo de Habilitadores na Prática

O exemplo 5 ilustra os habilitadores, suas interligações e as dimensões do habilitador, e como usá-los para benefício prático.

EXEMPLO 5 - HABILITADORES

Uma organização nomeou ‘gerentes de processo’ de TI, encarregados de definir e operar processos de TI eficientes e eficazes, no contexto da boa governança e gestão de TI da organização.

Primeiramente, os gerentes de processo se concentraram no habilitador do processo, considerando as dimensões do habilitador:

Partes interessadas: Partes interessadas incluem todos os atores do processo, ou seja, todas as partes responsáveis, consultadas ou informadas (RACI) sobre, ou durante, as atividades do processo. Para tanto, a tabela RACI descrita no COBIT 5: Habilitador Processos poderá ser utilizada.

Metas: Cada processo deve definir metas adequadas e indicadores correspondentes. Por exemplo, para o processo Gerenciar Relacionamentos (processo APO08 do COBIT 5: Habilitador Processos) pode-se encontrar um conjunto de metas e indicadores de processo tais como:

- **Meta**: Bom entendimento, documentação e aprovação das estratégias, planos e requisitos do negócio.
  - **Métrica**: Percentual de programas alinhados com os requisitos/prioridades de negócios da organização.
- **Meta**: Existência de bons relacionamentos entre a organização e a área de TI.
  - **Métrica**: Classificações de usuário e pesquisas de satisfação do pessoal de TI.

Ciclo de Vida: Cada processo tem um ciclo de vida, ou seja, ele deve ser criado, executado, monitorado e ajustado conforme necessário. Eventualmente, o processo deixa de existir. Neste caso, os gerentes de processo terão de conceber e definir o processo primeiro. Eles podem usar vários elementos do COBIT 5: Habilitador Processos para conceber os processos, ou seja, definir responsabilidades e desmembrar o processo em práticas e atividades, bem como definir os produtos do trabalho do processo (entradas e saídas). Em um segundo momento, o processo deverá ser criado de forma mais sólida e eficiente e para isso os gerentes de processo podem elevar o nível de capacidade do processo. O Modelo de Capacidade de Processo do COBIT 5 inspirado no ISO/IEC 15504 e os atributos de capacidade do processo podem ser usados para essa finalidade.

EXEMPLO 5 – HABILITADORES (CONT)
Boa prática: O COBIT 5 descreve de forma bastante detalhada as boas práticas de processos no COBIT 5: Habilitador Processos, conforme mencionado no item anterior. Inspiração e exemplos de processos podem ser encontrados ali, cobrindo todo o espectro de atividades necessárias para a boa governança e gestão corporativa de TI.
Além de orientação sobre o habilitador de processo, os gerentes de processo podem decidir observar diversos outros habilitadores tais como:
As tabelas RACI, que descrevem as funções e responsabilidades. Outros habilitadores permitem aprofundar-se nesta dimensão, tais como:
No habilitador competências e habilidades, as que são necessárias em cada função podem ser definidas com metas apropriadas (ex: níveis de habilidade técnica e comportamental) e seus respectivos indicadores podem ser definidos.
A tabela RACI também contém diversas estruturas organizacionais. Essas estruturas podem ser mais bem elaboradas no habilitador estruturas organizacionais, onde uma descrição mais detalhada da estrutura pode ser encontrada, resultados esperados e seus respectivos indicadores podem ser definidos (ex: decisões) e boas práticas podem ser definidas (ex: abrangência do controle, princípios operacionais da estrutura, nível de autoridade).
Princípios e políticas formalizarão os processos e prescreverão porque o processo existe, a quem se aplica e como o processo deverá ser usado. Esta é a área de enfoque do habilitador de políticas e princípios.

O Apêndice G discute as sete categorias de habilitadores com mais detalhes. Recomenda-se a leitura deste Apêndice para melhor entendimento dos habilitadores e de quão poderosos eles podem ser na organização da governança e gestão corporativa de TI.

CAPÍTULO 6
5º PRINCÍPIO: DISTINGUIR A GOVERNANÇA DA GESTÃO

Governança e Gestão

O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas abrangem diversos tipos de atividades, requerem diferentes estruturas organizacionais e atendem a propósitos diferentes. O ponto de vista do COBIT 5 sobre esta fundamental distinção entre governança e gestão é:

- Governança

A governança garante que as necessidades, condições e opções das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.

Na maioria das organizações, a governança geral é de responsabilidade do conselho de administração sob a liderança do presidente.

- Gestão

A gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.

Na maioria das organizações, a gestão é de responsabilidade da diretoria executiva sob a liderança do diretor executivo (CEO).

Interações Entre Governança e Gestão

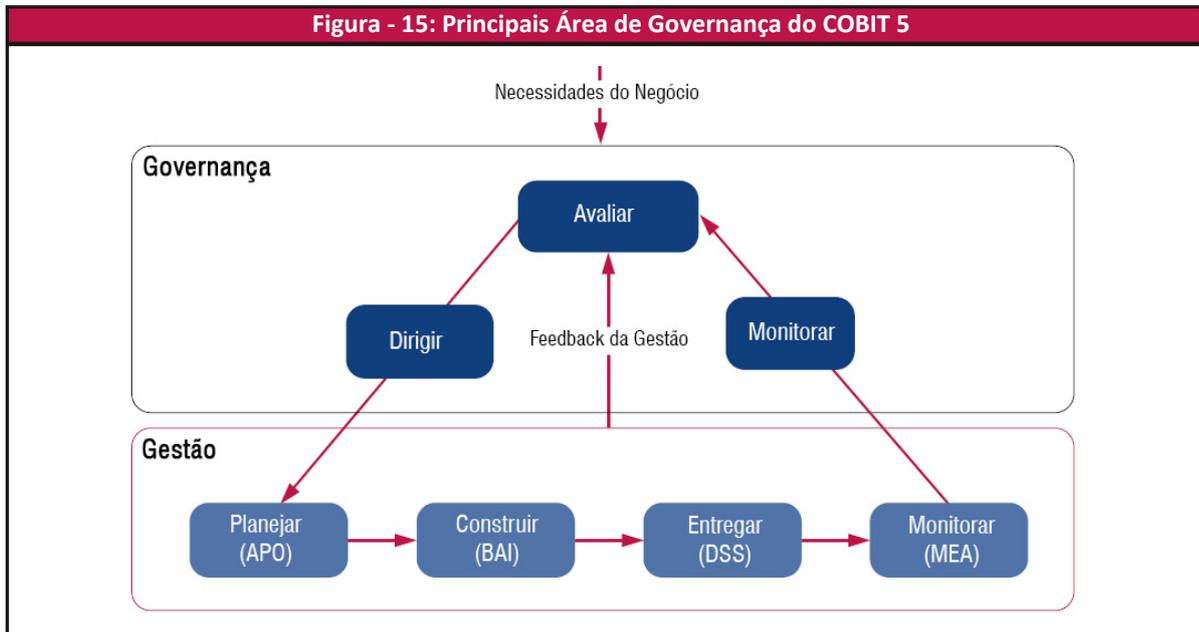
A partir das definições de governança e gestão, fica claro que elas incluem diversos tipos de atividades, com diferentes responsabilidades; entretanto, dado o papel da governança - de avaliar, orientar e monitorar - uma série de interações é exigida entre a governança e a gestão a fim de resultar um eficiente e eficaz sistema de governança. Essas interações, usando a estrutura de habilitadores, são apresentadas em um alto nível na figura 14.

Figura - 14: Interações entre Governança e Gestão

Habilitador	Interação Governança e Gestão
Processos	A ilustração do modelo de processo do COBIT 5 (COBIT 5: Habilitador Processos) faz uma distinção entre processos de governança e de gestão, inclusive com conjuntos específicos de práticas e atividades de cada um. O modelo de processo também inclui as tabelas RACI, que descrevem as responsabilidades das diferentes estruturas organizacionais e suas funções na organização.
Informação	O modelo de processo descreve entradas e saídas das diferentes práticas do processo para outros processos, inclusive as informações trocadas entre os processos de governança e de gestão. Informações usadas para avaliar, orientar e monitorar a TI da organização são trocadas entre a governança e a gestão conforme descrição nas entradas e saídas do modelo de processo.
Estruturas organizacionais	Diversas estruturas organizacionais são definidas em cada organização; estruturas podem ser definidas no âmbito da governança ou no âmbito da gestão, dependendo da sua composição e do escopo das decisões. Pelo fato da governança definir a orientação, há uma interação entre as decisões tomadas pelas estruturas de governança – ex: decisão sobre o portfólio de investimentos e a definição do apetite ao risco – e as decisões e operações que implementam as primeiras.
Princípios, políticas e modelos	Princípios, políticas e modelos são os veículos pelo qual as decisões de governança são institucionalizadas na organização, e por esse motivo constituem uma interação entre as decisões de governança (definição da orientação) e a gestão (execução das decisões).
Cultura, ética e comportamento	O comportamento também é um habilitador essencial da boa governança e gestão da organização. Ele fica no topo – liderando por exemplos – e é, portanto, uma interação importante entre a governança e a gestão.
Pessoas, habilidades e competências	As atividades de governança e gestão requerem conjuntos de habilidades diferentes, mas uma habilidade essencial para os membros do órgão de governança e de gestão é entender as duas tarefas e como elas se diferenciam.
Serviços, infraestrutura e aplicativos	Serviços são necessários, apoiados por aplicativos e infraestrutura que proporcionem ao órgão de governança informações adequadas e apoio às seguintes atividades da governança: avaliação, definição da orientação e monitoramento.

Modelo de Referência de Processo do COBIT 5

O COBIT 5 não é prescritivo, mas defende que as organizações implementem os processos de governança e gestão de tal forma que as principais áreas sejam cobertas, conforme demonstrado na figura 15.

Figura - 15: Principais Área de Governança do COBIT 5

Uma organização pode organizar seus processos conforme julgar conveniente, contanto que todos os objetivos de governança e gestão necessários sejam cobertos. Organizações de menor porte podem ter menos processos; organizações de maior porte e mais complexas poderão ter muitos processos, todos para cobrir os mesmos objetivos.

O COBIT 5 inclui um modelo de referência de processo, que define e descreve em detalhes uma série de processos de governança e gestão. Ele representa todos os processos normalmente encontrados em uma organização relacionados às atividades de TI, fornecendo um modelo de referência comum compreensível para os gerentes operacionais de TI e de negócios. O modelo de processo proposto é um modelo completo e abrangente, mas não é o único modelo de processo possível. Cada organização deverá definir seu próprio conjunto de processos, levando em consideração sua situação específica.

Incorporar um modelo operacional e uma linguagem comum para todas as partes da organização envolvidas com atividades de TI é uma das etapas mais importantes e críticas da boa governança. Também oferece um modelo para medir e monitorar o desempenho de TI, promovendo garantia (*assurance*) da TI, comunicação com os provedores de serviço e melhor integração com as práticas da administração.

O modelo de referência de processo do COBIT 5 divide os processos de governança e gestão de TI da organização em dois domínios de processo principais:

- **Governança** - Contém cinco processos de governança; e dentro de cada processo são definidas práticas para Avaliar, Dirigir e Monitorar (*Evaluate, Direct and Monitor* - EDM)[5].
- **Gestão** - Contém quatro domínios, em consonância com as áreas responsáveis por planejar, construir, executar e monitorar (*Plan, Build, Run and Monitor* - PBRM), e oferece cobertura de TI de ponta a ponta. Esses domínios são uma evolução do modelo de processos e domínios do COBIT 4.1. Os nomes dos domínios foram escolhidos em consonância com as designações dessas áreas principais, e usam mais verbos para descrevê-las:
  - Alinhar, Planejar e Organizar (*Align, Plan and Organise* – (APO)
  - Construir, Adquirir e Implementar (*Build, Acquire and Implement* – (BAI)
  - Entregar, Serviços e Suporte (*Deliver, Service and Support* - (DSS)
  - Monitorar, Avaliar e Analisar (*Monitor, Evaluate and Assess* – (MEA)

Cada domínio contém diversos processos. Embora, conforme descrito previamente, a maioria dos processos requeira atividades para ‘planejar’, ‘construir’, ‘entregar’ e ‘monitorar’ o processo ou problema específico que está sendo tratado (por exemplo, qualidade, segurança), eles são alocados em domínios de acordo com a área de atividade mais relevante quando TI é analisada em nível corporativo.

O modelo de referência de processo do COBIT 5 é o sucessor do modelo de processo do COBIT 4.1, e conta ainda com a integração dos modelos de processo do Risk IT e Val IT.

A figura 16 mostra o conjunto completo dos 37 processos de governança e de gestão do COBIT 5. Os detalhes de todos os processos, de acordo com o modelo de processo descrito previamente, foram incluídos no COBIT 5: Habilitador Processos.

---

[5] No contexto do domínio de governança, ‘monitorar’ significa as atividades em que o órgão de governança verifica em que medida a orientação definida para a gestão foi efetivamente aplicada.

Figura - 16: Modelo de Referência de Processo do COBIT 5

Processos de Governança Corporativa de TI

Avaliar, Dirigir e Monitorar

EDM01 Garantir a Definição e Manutenção do Modelo de Governança

EDM02 Garantir a Realizacao de Beneficios

EDM03 Garantir a Otimização do Risco

EDM04 Garantir a Otimização dos Recursos

EDM 05 Garantir Transparência para as Partes Interessadas

Alinhar, Planejar e Organizar

APO01 Gerenciar a Estrutura de Gestao de TI

APO02 Gerenciar a Estrategia

APO03 Gerenciar Arquitetura da Organizacao

APO04 Gerenciar Inovação

APO05 Gerenciar Portfolio

APO06 Gerenciar Orcamento e Custos

APO07 Gerenciar Recursos Humanos

APO08 Gerenciar Relacionamentos

APO09 Gerenciar Contratos de Prestação de Serviços

APO10 Gerenciar Fornecedores

APO11 Gerenciar Qualidade

APO12 Gerenciar Riscos

APO13 Gerenciar Segurança

Construir, Adquirir e Implementar

BAI01 Gerenciar Programas e Projetos

BAI02 Gerenciar Definição de Requisitos

BAI03 Gerenciar Identificacao e Desenvolvimento de Solucoes

BAI04 Gerenciar Disponibilidade e Capacidade

BAI05 Gerenciar Capacidade de Mudanca Organizacional

BAI06 Gerenciar Mudancas

BAI07 Gerenciar Aceitacao e Transicao da Mudanca

BAI08 Gerenciar Conhecimento

BAI09 Gerenciar Ativos

BAI10 Gerenciar Configuracao

Entregar, Serviço e Suporte

DSS01 Gerenciar Operações

DSS02 Gerenciar Solicitações e Incidentes de Serviços

DSS03 Gerenciar Problemas

DSS04 Gerenciar Continuidade

DSS05 Gerenciar Serviços de Segurança

DSS06 Gerenciar Controles do Processo de Negócio

Monitorar, Avaliar e Analisar

MEA01 Monitorar, Avaliar e Analisar Desempenho e Conformidade

MEA02 Monitorar, Avaliar e Analisar o Sistema de Controle Interno

MEA03 Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos

Processos para Gestão Corporativa de TI

CAPÍTULO 7
GUIA DE IMPLEMENTAÇÃO

Introdução

O valor ótimo pode ser realizado a partir da aplicação do COBIT somente se ele tiver sido efetivamente adotado e adaptado para atender ao ambiente único de cada organização. Cada abordagem de implementação também deverá abordar desafios específicos, inclusive a gestão de mudanças de cultura e comportamento.

A ISACA oferece orientação prática e ampla à implementação em sua publicação **COBIT 5 Implementação**[6], que se baseia em um ciclo de vida de melhoria contínua. Não pretende ser uma abordagem prescritiva nem uma solução completa, mas sim um guia para evitar as armadilhas geralmente encontradas, aplicar boas práticas e apoiar no atingimento de resultados positivos. O guia também é apoiado por um kit de ferramentas de implementação que contém uma variedade de recursos que serão continuamente aperfeiçoados. Seu conteúdo inclui:

- Ferramentas de autoavaliação, medição e diagnóstico
- Apresentações destinadas a diversos públicos
- Artigos relacionados e explicações adicionais

O objetivo deste capítulo é apresentar a implementação e o ciclo de vida de melhoria contínua em um alto nível e destacar diversos tópicos importantes do **COBIT 5 Implementação** tais como:

- Elaborar um estudo de caso para a implementação e melhoria da governança e gestão de TI
- Reconhecer os pontos fracos mais comuns e os eventos desencadeadores
- Criar o ambiente apropriado para a implementação
- Aplicar o COBIT para identificar falhas e orientar o desenvolvimento de habilitadores tais como políticas, processos, princípios, estruturas organizacionais bem como funções e responsabilidades

Considerar o Contexto da Organização

A governança e gestão corporativa de TI organização não ocorre no vácuo. Cada organização deve elaborar seu próprio plano ou roteiro de implementação, dependendo de fatores específicos do ambiente interno e externo da organização tais como:

- Ética e cultura
- Leis, regulamentos e políticas aplicáveis
- Missão, visão e valores
- Políticas e práticas de governança
- Plano de negócios e intenções estratégicas
- Modelo operacional e nível de maturidade
- Estilo de gestão
- Apetite ao risco (*risk appetite*)
- Capacidades e recursos disponíveis
- Práticas da indústria

É igualmente importante aproveitar para aprimorar com base nos atuais habilitadores de governança corporativa.

A abordagem ideal à governança e gestão corporativa de TI organização será diferente para cada organização e o contexto deve ser entendido e considerado a fim de adotar e adaptar o COBIT com eficiência na implementação dos habilitadores de governança e gestão de TI da organização. O COBIT é muitas vezes sustentado por outros modelos, boas práticas e padrões, e estes, por sua vez, também devem ser adaptados de modo a atender requisitos específicos.

Os principais fatores para uma implementação bem-sucedida incluem:

- Fornecimento pela alta administração da orientação e da ordem para a iniciativa, bem como o compromisso e o apoio visíveis e contínuos
- Apoio aos processos de governança e gestão por todas as partes a fim de entender os objetivos de TI e os da organização
- Garantia de comunicação efetiva e capacitação das mudanças necessárias
- Adaptação do COBIT e demais padrões e boas práticas de apoio a fim de atender ao contexto único da organização
- Foco em resultados rápidos e priorização das melhorias mais benéficas que são mais fáceis de implementar

Criar o Ambiente Apropriado

É importante que a implementação de iniciativas utilizando COBIT seja devidamente governada e adequadamente gerenciada. Importantes iniciativas de TI geralmente falham devido à orientação, apoio e supervisão inadequados dos diversos envolvidos, e com a implementação da governança ou gestão dos habilitadores de TI através do COBIT não é diferente. Apoio e orientação das principais partes interessadas são críticos para que as melhorias sejam adotadas e mantidas.

[6] *www.isaca.org/cobit*

Em um ambiente corporativo fraco (como um modelo operacional geral de negócios pouco claro ou falta de habilitadores de governança em nível corporativo) este apoio e participação são ainda mais importantes.

Os habilitadores que aplicam o COBIT devem fornecer uma solução que trate das necessidades e problemas reais da organização, em vez de servir como fins em si mesmos. Requisitos baseados nos pontos fracos e nas tendências atuais devem ser identificados e aceitos pela administração como áreas a serem tratadas. Verificações de integridade, diagnósticos ou avaliações de capacidade em alto nível baseadas no COBIT são excelentes ferramentas para aumentar a sensibilização, criar consenso e gerar um compromisso de ação. O compromisso e a adesão das partes interessadas pertinentes devem ser solicitados desde o início. Para alcançar isto, os objetivos e benefícios da implementação devem ser claramente expressos em termos de negócio e resumidos em um breve estudo de caso.

Após o compromisso ter sido obtido, os recursos adequados deverão ser fornecidos para apoiar o programa. As principais funções e responsabilidades do programa deverão ser definidas e atribuídas. Cuidados deverão ser sempre tomados para a manutenção do compromisso de todas as partes interessadas afetadas.

Estruturas e processos apropriados para supervisão e orientação deverão ser criados e mantidos. Essas estruturas e processos também deverão garantir o alinhamento contínuo das abordagens de governança e gestão de risco em toda a organização.

Apoio e compromisso visíveis devem ser oferecidos pelas principais partes interessadas tais como a diretoria e os executivos para definir a 'mais alta sintonia' e garantir o compromisso com o programa em altos níveis.

Reconhecer Pontos de Dor e Eventos Desencadeadores

Há diversos fatores que podem indicar a necessidade de melhorar a governança e gestão corporativa de TI.

Usando os pontos de dor ou eventos desencadeadores como ponto de partida para as iniciativas de implementação, o estudo de caso de melhoria da governança ou gestão corporativa de TI pode estar relacionado aos problemas práticos ou cotidianos sendo vivenciados. Isto aumentará a adesão e criará o senso de urgência na organização necessário para iniciar a implementação. Além disso, resultados rápidos podem ser identificados e o valor agregado pode ser demonstrado nas áreas da organização mais visíveis ou reconhecíveis. Isto cria uma plataforma para a introdução de novas mudanças e pode ajudar na obtenção do compromisso e apoio de toda a administração sênior para mudanças mais profundas.

Exemplos de alguns dos pontos de dor mais comuns para os quais os habilitadores de governança ou gestão de TI novos ou revisados podem ser a solução (ou parte da solução), conforme identificados no COBIT 5 Implementação, são:

- Frustração da organização com iniciativas fracassadas, aumentando os custos de TI e a percepção de baixo valor para o negócio
- Incidentes significativos relacionados ao risco de TI para o negócio, tais como perda de dados ou falha em projetos
- Problemas com a terceirização da prestação de serviços, tais como o não cumprimento de forma consistente dos níveis de serviço acordados
- Não cumprimento das exigências regulatórias ou contratuais
- Limitações de TI na capacidade de inovação e agilidade dos negócios da organização
- Descobertas das auditorias regulares sobre o fraco desempenho de TI ou relatórios de problemas com a qualidade de TI
- Gastos com TI ocultos e não autorizados
- Duplicação ou sobreposição das iniciativas ou desperdício de recursos
- Recursos de TI insuficientes, pessoal com competências inadequadas ou insatisfação ou esgotamento do pessoal
- Mudanças relacionadas com a TI que não atendem às necessidades da organização e demoram a dar retorno ou estouram o orçamento
- Membros da diretoria, executivos ou gerentes seniores que relutam em se envolver com TI, ou falta de patrocinadores comprometidos e satisfeitos para área de TI da organização
- Múltiplos e complexos modelos operacionais de TI

Além desses pontos de dor, outros eventos em ambientes internos e externos à organização podem sinalizar ou desencadear um foco na governança e gestão de TI. Exemplos do capítulo 3 da publicação COBIT 5 Implementação são:

- Fusão, aquisição ou alienação
- Uma mudança no mercado, posição econômica ou competitiva
- Mudança no modelo operacional do negócio ou acordos de terceirização
- Nova regulamentação ou requisitos de conformidade
- Mudança significativa de tecnologia ou de paradigma
- Foco ou projeto de governança em toda a organização
- Novo CEO, CFO, CIO, etc.
- Auditoria externa ou avaliações de consultores
- Uma nova estratégia ou de negócio

Capacitar a Mudança

O sucesso da implementação depende da implantação da mudança adequada (dos habilitadores da governança ou gestão apropriados) de forma correta. Em muitas organizações, há um foco significativo no primeiro aspecto - núcleo de governança ou gestão de TI - mas há pouca ênfase na gestão dos aspectos humanos, comportamentais e culturais da mudança e motivação das partes interessadas para aceitar a mudança.

Não se deve pressupor que as várias partes interessadas envolvidas com os habilitadores novos ou revisados, ou afetados por eles, os aceitarão prontamente e adotarão a mudança. A possibilidade de ignorarem e/ou resistirem à mudança deve ser

tratada por meio de uma abordagem estruturada e proativa. Além disso, a conscientização ideal do programa de implementação deve ser alcançada através de um plano de comunicação eficiente que defina o que será comunicado, de que forma e por quem, ao longo das várias fases do programa.

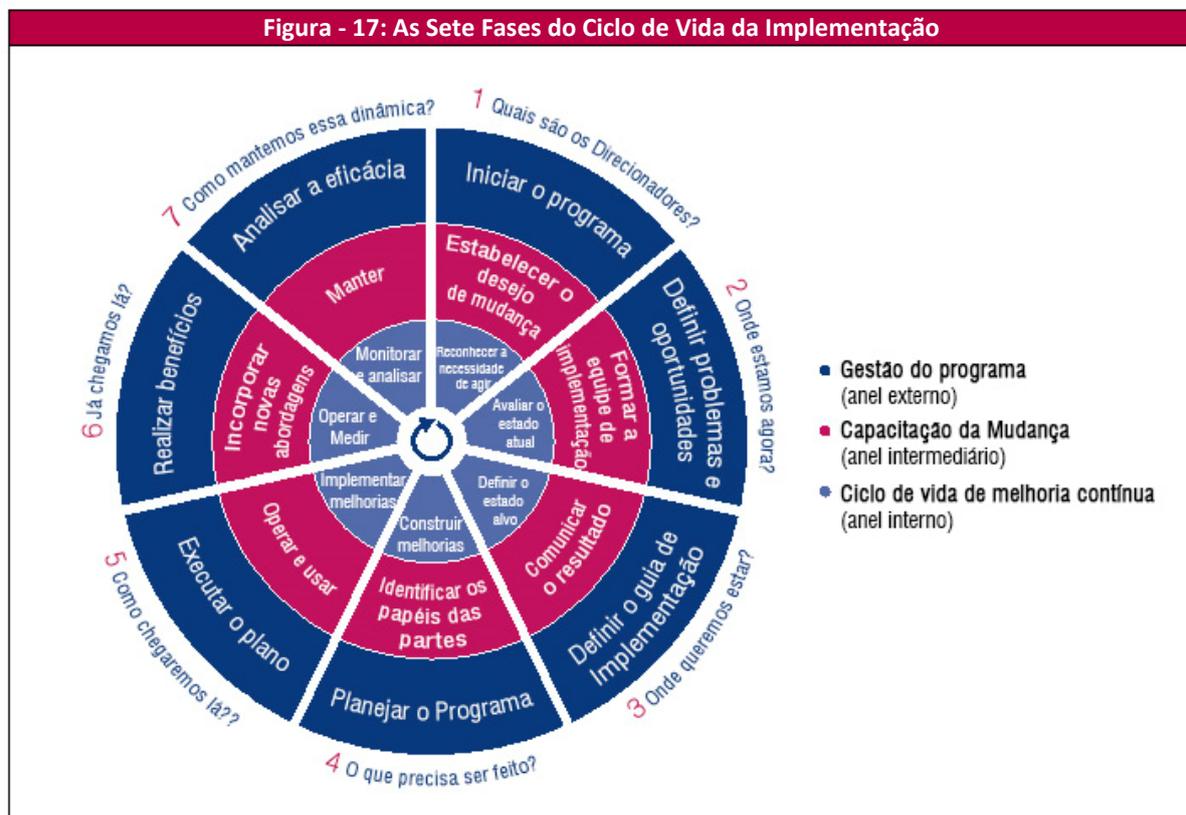
Melhoria sustentável pode ser conseguida obtendo-se o compromisso das partes interessadas (investimento na conquista de corações e mentes, do tempo dos líderes, e na comunicação e resposta à força de trabalho) ou, se ainda for necessário, aplicando-se em conformidade (investimento em processos para administrar, monitorar e executar). Em outras palavras, as barreiras humanas, comportamentais e culturais devem ser superadas de modo que haja um interesse comum em adotar corretamente a mudança, infundir a vontade de adotar a mudança e garantir a capacidade de adotar a mudança.

Uma Abordagem ao Ciclo de Vida

O ciclo de vida da implementação apresenta uma forma das organizações usarem o COBIT para tratar da complexidade e os desafios geralmente encontrados durante as implementações. Os três componentes inter-relacionados do ciclo de vida são:

1. Ciclo de vida principal de melhoria contínua - Este não é um projeto isolado.
2. Capacitação da mudança - Abordagem dos aspectos comportamentais e culturais
3. Gestão do programa

Como já discutido, o ambiente adequado deve ser criado para garantir o sucesso da implementação ou da iniciativa de melhoria. O ciclo de vida e suas sete fases são ilustrados na **figura 17**.

Figura - 17: As Sete Fases do Ciclo de Vida da Implementação

A **1ª Fase** começa com o reconhecimento e aceitação da necessidade de uma implementação ou iniciativa de implementação. Ela identifica os atuais pontos fracos e desencadeadores e cria um desejo de mudança nos níveis de gestão executiva.

A **2ª Fase** concentra-se na definição do escopo da implementação ou da iniciativa de implementação usando o mapeamento dos objetivos corporativos do COBIT em objetivos de TI e nos respectivos processos de TI, e considerando também como os cenários de risco poderiam destacar quais os principais processos que se deve concentrar. Diagnósticos de alto nível também podem ser úteis para definir o escopo e compreender as áreas com alta prioridade que se deve concentrar. Uma avaliação do estado atual é então realizada, e os problemas ou deficiências são identificados realizando-se uma avaliação da capacidade do processo. Iniciativas em larga escala devem ser estruturadas como múltiplas interações do ciclo de vida - para qualquer iniciativa de implementação superior a seis meses há um risco de perda da dinâmica, foco e adesão das partes interessadas.

Durante a **3ª Fase**, uma meta de melhoria é definida, seguida por uma análise mais detalhada, que alavanca a orientação do COBIT, a fim de identificar falhas e possíveis soluções. Algumas soluções podem apresentar resultados rápidos enquanto outras poderão exigir atividades mais desafiadoras em um prazo maior. Prioridade deve ser dada às iniciativas mais fáceis de alcançar e que provavelmente produzirão os melhores benefícios.

A **4ª Fase** planeja soluções práticas através da definição de projetos apoiados por estudos de casos justificáveis. Um plano de mudança para a implementação também é desenvolvido nesta fase. Um estudo de caso bem desenvolvido ajuda a garantir que os benefícios do projeto sejam identificados e monitorados.

As soluções propostas são implementadas na forma de práticas diárias na **5ª Fase**. Medições podem ser definidas e o monitoramento estabelecido com o uso das metas e indicadores do COBIT para garantir que o alinhamento da organização seja atingido e mantido e o desempenho possa ser medido. O sucesso exige demonstração de envolvimento e empenho pela alta administração, bem como a responsabilidade dos envolvidos das áreas de TI e de administração.

A **6ª Fase** concentra-se na operação sustentável dos habilitadores novos ou aperfeiçoados e no monitoramento do atingimento dos benefícios esperados.

Durante a **7ª Fase**, o sucesso da iniciativa como um todo é analisado, novos requisitos para a governança ou gestão de TI da organização são identificados e a necessidade de melhoria contínua é reforçada.

Com o tempo, o ciclo de vida deve ser seguido de forma interativa paralelamente à criação de uma abordagem sustentável para a governança e gestão de TI da organização.

Primeiros Passos: Elaborar o Estudo de Caso

Para garantir o sucesso das iniciativas de implementação que aplicam o COBIT, a necessidade de agir deve ser amplamente reconhecida e comunicada em toda a organização. Isto pode ser feito na forma de um ‘toque de despertar’ (onde pontos fracos estejam sendo vivenciados, conforme já discutido) ou uma expressão da oportunidade de melhoria a ser alcançada e, muito importante, dos benefícios que serão realizados. O nível adequado de urgência deve ser incutido e as principais partes interessadas devem estar cientes do risco de não tomar medidas bem como dos benefícios da realização do programa.

A iniciativa deve ser atribuída a um responsável, envolver todos as principais partes interessadas e basear-se em um estudo de caso. Inicialmente, isto pode ser feito em um alto nível do ponto de vista estratégico - de cima para baixo - começando com uma clara compreensão dos resultados organizacionais desejados e progredindo até uma descrição detalhada das tarefas e metas críticas, bem como das funções e responsabilidades. O estudo de caso é uma valiosa ferramenta de que dispõe a administração para orientação na criação de valor para a organização. O estudo de caso deve incluir, no mínimo, o seguinte:

- Os benefícios almejados para a organização, seu alinhamento com a estratégia de negócios e os respectivos responsáveis pelo benefício (que serão os responsáveis na organização pela sua garantia). Isto pode basear-se em pontos fracos e eventos desencadeadores.
- As mudanças nos negócios necessárias para criar o valor esperado. Isto pode basear-se em verificações de integridade e análises de falhas na capacidade e devem indicar claramente o que está incluído no escopo e o que não está.
- Os investimentos necessários para criar as mudanças na governança e gestão de TI da organização (com base nas estimativas dos projetos necessários)
- Os custos fixos do negócio e de TI
- Os benefícios esperados da operação após a mudança
- O risco inerente nos pontos acima, inclusive quaisquer restrições ou dependências (com base nos desafios e fatores de sucesso)
- Funções e responsabilidades relacionadas à iniciativa
- Como o investimento e a criação de valor serão monitorados durante todo o ciclo de vida econômico, e como os indicadores serão usadas (com base nas metas e resultados)

O estudo de caso não é um documento estático definitivo, mas uma ferramenta operacional dinâmica que deve ser continuamente atualizada para refletir a atual visão do futuro para que uma visão da viabilidade do programa possa ser mantida.

Pode ser difícil quantificar os benefícios da implementação ou das iniciativas de implementação e cuidados deverão ser tomados para comprometimento somente com benefícios realistas e atingíveis. Estudos realizados em diversas organizações podem oferecer informações úteis sobre os benefícios que foram alcançados.

EXEMPLO 6 – ESTATÍSTICAS DE GOVERNANÇA E TI

ITGI encomendou uma pesquisa de mercado sobre a governança de TI[7] à PwC, com mais de 800 profissionais de TI e de negócios entrevistados em 21 países, e 38% dos entrevistados citaram a redução dos custos de TI como resultado da governança das práticas de TI, 28,1% citaram a melhoria da competitividade da organização e 27,1% indicaram melhor retorno dos investimentos em TI. Além disso, diversos benefícios menos tangíveis foram relatados tais como a melhoria da gestão do risco de TI (42,2% dos entrevistados), melhor comunicação e relacionamentos entre as áreas administrativas e de TI (39,6% dos entrevistados) e melhoria na execução de TI para atingimento dos objetivos corporativos (37,3% dos entrevistados).

A ISACA também tem conduzido pesquisas[8] que exploram e demonstram o valor do COBIT para a organização. O conjunto de dados resultante da pesquisa oferece muitas oportunidades de análise e esclarece o relacionamento entre a governança corporativa de TI e o desempenho da organização.

Outro estudo realizado com 250 organizações em todo o mundo descobriu que as organizações com melhor governança de TI tiveram uma rentabilidade pelo menos 20% maior do que aquelas com fraca governança, considerando-se os mesmos objetivos.[9] Argumenta-se que o valor de TI da organização derive diretamente da eficiência na governança de TI.

Por fim, outro estudo de caso no setor aéreo concluiu que a implementação e a garantia contínua da governança corporativa de TI restauraram a confiança entre o negócio e TI, e isso resultou em um alinhamento maior dos investimentos para os objetivos estratégicos. Além disso, benefícios mais tangíveis foram relatados neste estudo, inclusive a redução do custo fixo de TI por unidade de produção comercial, e a liberação de fundos para a inovação. Outro estudo multicasos no setor financeiro demonstrou que as organizações com melhores abordagens à governança de TI claramente obtiveram as maiores pontuações de maturidade do alinhamento entre o negócio e TI.[10]

---

[7] ITGI, Global Status Report on the Governance of Enterprise IT (GEIT) — 2011, EUA, 2011, www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Global-Status-Report-on-the-Governance-of-Enterprise-IT-GEIT-2011.aspx

[8] ISACA, Building the Business Case for COBIT® and Val ITTM Executive Briefing, EUA, 2009, www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Building-the-Business-Case-for-COBIT-and-Val-IT-Executive-Briefing.aspx

[9] Weill, Peter; Jeanne W. Ross; IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, EUA, 2004

[10] De Haes, Steven; Dirk Gemke; John Thorp; Wim Van Grembergen; 'Analyzing IT Value Management @ KLM Through the Lens of Val IT', ISACA Journal, 2011, vol 4. Van Grembergen, Wim; Steven De Haes; Enterprise Governance of IT: Achieving Alignment and Value, Springer, EUA, 2009

CAPÍTULO 8
MODELO DE CAPACIDADE DE PROCESSO DO COBIT 5

Introdução

Usuários do COBIT 4.1, Risk IT e Val IT estão familiarizados com os modelos de maturidade de processo incluídos naqueles modelos. Estes modelos são usados para medir a maturidade atual ou 'no estado em que se encontra' dos processos de TI de uma organização para definir o estado de maturidade 'necessário' e para determinar a diferença entre eles e como melhorar o processo para atingir o nível de maturidade desejado.

O conjunto de produtos COBIT 5 inclui um modelo de capacidade de processo, com base no padrão de Avaliação de Processo – Engenharia de Software ISO/IEC 15504 reconhecido internacionalmente. Este modelo atingirá os mesmos objetivos gerais de avaliação de processo e apoio à melhoria do processo, ou seja, ele proporcionará meios para medir o desempenho de qualquer um dos processos de governança (baseados em EDM) ou processos de gestão (baseados em PBRM) e permitirá a identificação das áreas que precisam ser melhoradas.

No entanto, o novo modelo é diferente do modelo de maturidade do COBIT 4.1 em seu projeto e aplicação, e por essa razão, os seguintes tópicos serão discutidos:

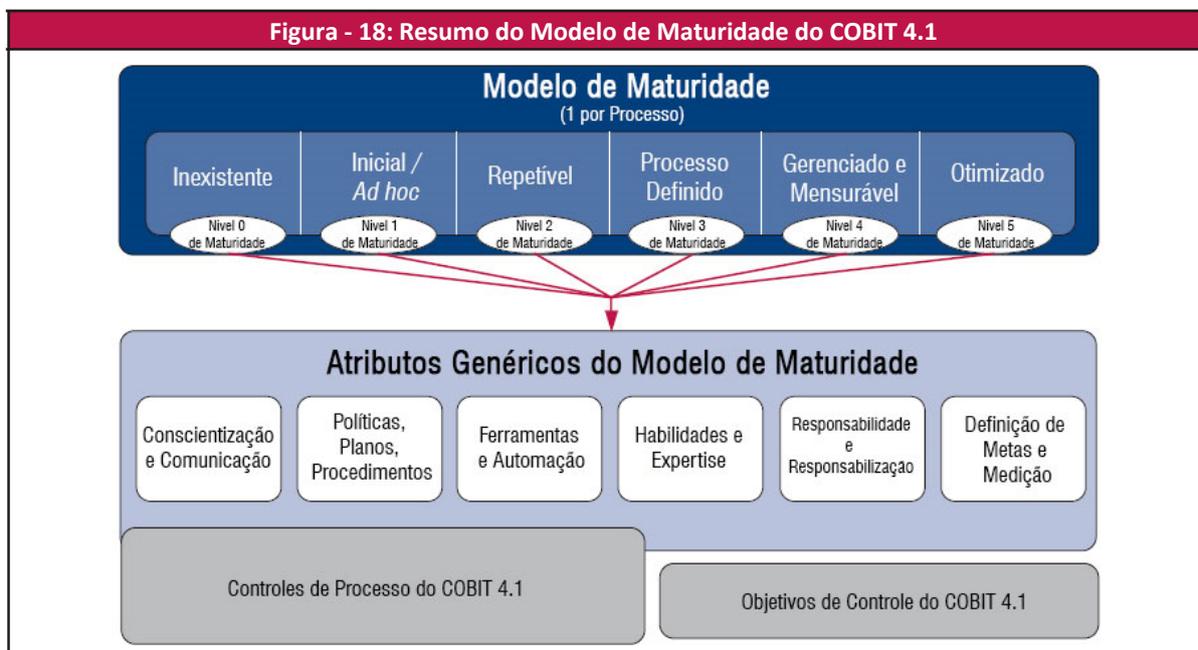
- Diferenças entre os modelos do COBIT 5 e do COBIT 4.1
- Benefícios do modelo do COBIT 5
- Resumo das diferenças que os usuários do COBIT 5 encontrarão na prática
- Avaliação de capacidade do COBIT 5

Detalhes da abordagem da avaliação de capacidade do COBIT 5 foram incluídos na publicação COBIT® *Process Assessment Mode*l (PAM): *Using* COBIT® 4.1[11] da ISACA.

Embora esta abordagem forneça informações valiosas sobre o estado dos processos, os processos são apenas um dos sete habilitadores de governança e gestão. Consequentemente, as avaliações de processo não apresentarão o quadro completo do estado de governança de uma organização. Para tanto, os demais habilitadores também devem ser avaliados.

Diferenças Entre o Modelo de Maturidade do COBIT 4.1 e o Modelo de Capacidade de Processo do COBIT 5

Os elementos da abordagem do modelo de maturidade do COBIT 4.1 são demonstrados na figura 18.

Figura - 18: Resumo do Modelo de Maturidade do COBIT 4.1

Usar o modelo de maturidade do COBIT 4.1 para fins de melhoria no processo - avaliar a maturidade de um processo, definir o nível de maturidade desejado e identificar as falhas - necessárias com o uso dos seguintes componentes do COBIT 4.1:

- Primeiro, uma avaliação deverá ser realizada para confirmar se os objetivos de controle do processo foram atingidos.
- Em seguida, o modelo de maturidade incluído na diretriz de gestão de cada processo pode ser utilizado na obtenção do perfil de maturidade do processo.

[11] *www.isaca.org/cobit-pam*

- Além disso, o modelo de maturidade genérico do COBIT 4.1 fornece seis atributos distintos aplicáveis para cada processo e que auxiliaram na obtenção de uma visão mais detalhada do nível de maturidade dos processos.
- Controles de processo são objetivos de controle genéricos – eles também devem ser analisados quando um processo de avaliação for realizado. Controles de processo sobrepõem-se parcialmente aos atributos genéricos do modelo de maturidade.

A abordagem da capacidade de processo do COBIT 5 pode ser resumida conforme demonstrado na figura 19.

Figura - 19: Resumo do Modelo de Capacidade de Processo do COBIT 5

Atributos Genéricos de Capacidade de Processo

Atributos de Execução (PA) 1.1 Execução do Processo
PA 2.1 Gestão da Execução
PA 2.2 Gestão dos Produtos de Trabalho
PA 3.1 Definição do Processo
PA 3.2 Implementação do Processo
PA 4.1 Gestão do Processo
PA 4.2 Controle do Processo
PA 5.1 Inovação do Processo
PA 5.2 Otimização do Processo

Processo Inexistente 0
Processo Executado 1
Processo Gerenciado 2
Processo Estabelecido 3
Processo Previsível 4
Processo Otimizado 5

Modelo de Avaliação de Processo do COBIT 5 - Indicadores de Desempenho
Resultados do Processo
Práticas Básicas (Praticas de Governança / Gestão)
Produtos do Trabalho (Entradas / Saídas)

Modelo de Avaliação de Processo do COBIT 5 – Indicadores de Capacidade
Práticas Genéricas
Recursos Genéricos
Produtos de Trabalho Genéricos

Um processo pode atingir seis níveis de capacidade, incluindo uma designação de 'processo incompleto' caso suas práticas não atinjam o objetivo do processo:

- **0 Processo Incompleto** - O processo não foi implementado ou não atingiu seu objetivo. Neste nível, há pouca ou nenhuma evidência de qualquer atingimento sistemático do objetivo do processo.
- **1 Processo Executado** (um atributo) - O processo implementado atinge seu objetivo.
- **2 Processo Gerenciado** (dois atributos) - O processo realizado descrito acima agora é implementado de forma administrativa (planejado, monitorado e ajustado) e seus produtos do trabalho são adequadamente estabelecidos, controlados e mantidos.
- **3 Processo Estabelecido** (dois atributos) - O processo controlado descrito acima agora é implementado utilizando um processo definido capaz de atingir seus resultados.
- **4 Processo Previsível** (dois atributos) - O processo criado descrito acima opera agora dentro dos limites definidos para produzir seus resultados.
- **5 Processo Otimizado** (dois atributos) - O processo previsível descrito acima é continuamente melhorado visando o atingimento dos objetivos corporativos pertinentes, atuais ou previstos.

Cada nível de capacidade só pode ser atingido quando o nível anterior tiver sido plenamente alcançado. Por exemplo, uma capacidade de processo nível 3 (processo criado) exige que a definição do processo e os atributos de implantação do processo sejam amplamente atingidos depois que a capacidade dos atributos de processo do nível 2 forem atingidos (processo controlado).

Há uma diferença significativa entre a capacidade de processo nível 1 e os níveis de capacidade mais altos. O atingimento da capacidade de processo nível 1 exige que o atributo de desempenho do processo seja amplamente atingido, o que, de fato, significa que o processo está sendo realizado com sucesso e os resultados esperados estão sendo obtidos pela organização. Níveis de capacidade mais altos adicionam então diferentes atributos a ele. Neste esquema de avaliação, atingir a capacidade nível 1, mesmo em uma escala de 5, já pode ser considerado uma importante conquista para a organização. Observe que cada organização definirá (com base no custo-benefício e na viabilidade) sua meta ou nível desejado, que muito raramente será um dos mais altos.

As principais diferenças entre uma avaliação de capacidade de processo com base no ISO/IEC 15504 e no atual modelo de maturidade do COBIT 4.1 (e nos modelos de maturidade com base nos domínios Val IT e Risk IT semelhantes) podem ser resumidas conforme abaixo:

- A nomenclatura e o significado dos níveis de capacidade definidos para o ISO/IEC 15504 são ligeiramente diferentes dos atuais níveis de maturidade dos processos do COBIT 4.1.
- No ISO/IEC 15504, os níveis de capacidade são definidos por um conjunto de nove atributos de processo. Estes atributos abrangem alguns fundamentos cobertos pelos atuais atributos de maturidade e/ou controles de processos do COBIT 4.1, mas somente até certa medida e de uma maneira diferente.

Os requisitos do modelo de referência de processo em conformidade com o ISO/IEC 15504:2 determinam que na descrição de qualquer processo a ser avaliado, ou seja, qualquer processo de governança e/ou gestão do COBIT 5:

- O processo seja descrito em termos de seu objetivo e resultados.
- A descrição do processo não conterá nenhum aspecto da estrutura de medição além do nível 1, o que significa que nenhuma característica de um atributo de processo além do nível 1 poderá constar em na descrição de um processo. Se um processo for medido e monitorado, ou for formalmente descrito, etc., não poderá ser parte de uma descrição de processo ou de qualquer das práticas/ atividades de gestão abaixo. Isto significa que as descrições do processo - conforme incluídas no COBIT 5: Habilitador Processo - contêm somente os passos necessários para o atingimento das metas e objetivos do processo.
- Na sequência dos marcadores acima, os atributos comuns aplicáveis a todos os processos da organização, que produziram objetivos de controle duplicados na publicação do COBIT® *3rd Edition* e foram agrupados em objetivos de controle de processo (PC) do COBIT 4.1, agora foram definidos entre os níveis 2 e 5 do modelo de avaliação.

Diferenças na Prática[12]

A partir das descrições acima, fica claro que há algumas diferenças práticas associadas à mudança nos modelos de avaliação de processo. Os usuários devem ter ciência destas mudanças e estarem prontos para considera-las em seus planos de ação.

As principais mudanças a ser consideradas incluem:

- Embora seja tentador comparar os resultados da avaliação entre o COBIT 4.1 e o COBIT 5 por causa das aparentes semelhanças com o número de escalas e termos usados para descrevê-las, tal comparação é difícil por causa das diferenças no escopo, foco e intenção, conforme ilustrado na figura 20.
- No geral, as pontuações serão inferiores com o modelo de capacidade de processo do COBIT 5, conforme demonstrado na figura 20. No modelo de maturidade do COBIT 4.1, um processo poderia atingir o nível 1 ou 2 sem atingir plenamente todos os objetivos do processo; no nível de capacidade de processo do COBIT 5, isto resultará em uma pontuação mais baixa (0 ou 1).

As escalas de capacidade do COBIT 4.1 e do COBIT 5 podem ser consideradas para um ‘mapeamento’ aproximado, conforme demonstrado na figura 20.

- Não há mais um modelo de maturidade específico por processo no conteúdo do processo detalhado do COBIT 5 porque a abordagem da avaliação da capacidade de processo ISO/IEC 15504 não exige isso e ainda proíbe esta abordagem. Em vez disso, a abordagem define as informações requeridas no ‘modelo de referência de processo’ (o modelo de processo a ser utilizado na avaliação):
  - Descrição de processo, com as definições do objetivo
  - Práticas básicas, equivalentes às práticas de governança ou gestão de processo do COBIT 5
  - Produtos do trabalho, equivalentes às entradas e saídas do COBIT 5
- O modelo de maturidade do COBIT 4.1 produziu um perfil de maturidade de uma organização. O principal objetivo deste perfil era identificar em quais dimensões ou para quais atributos havia pontos fracos específicos que necessitavam de melhorias. Esta abordagem foi usada pelas organizações quando havia um foco na melhoria em vez da necessidade de obter um número de maturidade para fins de relatório. No COBIT 5 o modelo de avaliação fornece uma escala de medição para cada atributo de capacidade e orientação sobre como aplicá-la, então para cada processo uma avaliação pode ser feita para cada um dos nove atributos de capacidade.
- Os atributos de maturidade do COBIT 4.1 e os atributos de capacidade de processo do COBIT 5 não são idênticos. Eles sobrepõem-se/mapeiam até certa medida, conforme demonstrado na figura 21. As organizações que utilizam a abordagem dos atributos do modelo de maturidade do COBIT 4.1 podem reutilizar os atuais dados da sua avaliação e reclassificá-los segundo as avaliações de atributos do COBIT 5, com base na figura 21.

[12] Mais informações sobre o novo Programa de Avaliação do COBIT com base no ISO/IEC 15504 podem ser encontradas em: *www.isaca.org/cobit-assessment-programme*.

<table>
<tr><th colspan="3">Figura - 20: Tabela Comparativa Níveis de Maturidade (COBIT 4.1) e Níveis de Capacidade de Processo (COBIT 5)</th></tr>
<tr><th>Nível do Modelo de Maturidade do COBIT 4.1</th><th>Capacidade de Processo com Base no ISO/IEC 15504</th><th>Contexto</th></tr>
<tr><td>5 Otimizado – Os processos foram refinados ao nível de boa prática, com base nos resultados de melhorias contínuas e modelagem da maturidade com outras organizações. TI é aplicada de forma integrada para automatizar o fluxo de trabalho, oferecendo ferramentas para melhoria da qualidade e da eficácia, fazendo com que a organização se adapte rapidamente.</td><td>Nível 5: Processo Otimizado – O processo previsível, nível 4, é continuamente melhorado de modo a atender os objetivos corporativos pertinentes, atuais ou previstos.</td><td rowspan="3">Visão da Organização

Conhecimento Corporativo</td></tr>
<tr><td>4 Controlado e Mensurável – A administração monitora e mede a conformidade com os procedimentos e toma medidas quando parecer que os processos não estão funcionando efetivamente. Os processos estão em constante melhoria e resultam em boas práticas. Automação e ferramentas são utilizadas de maneira limitada ou fragmentada.</td><td>Nível 4: Processo Previsível – O processo Estabelecido, nível 3, opera agora com limites definidos, atingidos nos resultados do processo.</td></tr>
<tr><td>3 Processo Estabelecido – Os procedimentos foram padronizados, documentados e comunicados por meio de treinamento. Seguir esses processos é obrigatório; no entanto, é improvável que os desvios sejam detectados. Os procedimentos, por si só, não são sofisticados, mas são a formalização das práticas existentes.</td><td>Nível 3: Processo Estabelecido – O processo Gerenciado, nível 2, é agora implementado usando um processo definido capaz de atingir os resultados do processo.</td></tr>
<tr><td></td><td>Nível 2: Processo Gerenciado – O processo Executado, nível 1, é agora implementado de forma gerenciada (planejado, monitorado e ajustado) e seus produtos do trabalho são adequadamente estabelecidos, controlados e mantidos.</td><td rowspan="4">Visão de Instância

Conhecimento Individual</td></tr>
<tr><td>2 Repetível, mas intuitivo – Os processos se desenvolveram até o estágio em que procedimentos semelhantes são adotados por diferentes pessoas que realizam o mesmo trabalho. Não há treinamento formal ou comunicação de procedimentos padrão e a responsabilidade fica a critério do indivíduo. Há um alto grau de confiança no conhecimento das pessoas e, portanto, erros são possíveis.</td><td rowspan="2">Nível 1: Processo Executado – O processo implementado atinge a finalidade do processo.

Observação: É possível que alguns processos classificados como Modelo de Maturidade Nível 1 sejam classificados como nível 0 na ISO/IEC15504, se os resultados do processo não forem alcançados.</td></tr>
<tr><td>1 Inicial/Ad hoc – Há evidências de que a organização tenha reconhecido a existência de problemas que deveriam ser tratados. Contudo, não há processos padronizados; em vez disso, há abordagens ad hoc, que tendem a ser aplicadas individualmente ou com base em cada caso. A abordagem geral da gestão é desorganizada.</td></tr>
<tr><td>0 Inexistente – Completa falta de processos reconhecíveis. A organização nem sequer reconheceu que existe um problema a ser tratado.</td><td>Nível 0: Processo incompleto - O processo não foi implementado ou não cumpre sua finalidade.</td></tr>
</table>

Figura - 21: Tabela Comparativa Atributos de Maturidade (COBIT 4.1) e Atributos de Processo (COBIT 5)

Atributo de Maturidade do COBIT 4.1	Atributo de Capacidade de Processo do COBIT 5								
	Desempenho do Processo	Gestão de Desempenho	Gestão de Produto do Trabalho	Definição do Processo	Implementação do Processo	Gestão do Processo	Controle do Processo	Inovação do Processo	Otimização do Processo
Conscientização e Comunicação				■	■	■			
Políticas, planos e procedimentos							■		
Ferramentas e automação				■					
Habilidades e expertise				■	■				
Responsabilidade				■					
Definição de metas e medição		■				■			

Benefícios das Mudanças

Os benefícios do modelo de capacidade de processo do COBIT 5, comparados com os modelos de maturidade do COBIT 4.1 incluem:

- Maior ênfase no processo que está sendo realizado para confirmar que está efetivamente alcançando seus objetivos e os resultados esperados.
- Simplificação do conteúdo por meio da eliminação da duplicação, porque a avaliação do modelo de maturidade do COBIT 4.1 exigia o uso de diversos componentes específicos, inclusive o modelo de maturidade genérico, modelos de maturidades do processo, objetivos de controle e controles de processo para apoiar a avaliação do processo.
- Maior confiabilidade e repetitividade das atividades e análises da avaliação da capacidade do processo, reduzindo debates e desentendimentos entre as partes interessadas em relação aos resultados da avaliação.
- Maior uso dos resultados da avaliação da capacidade do processo, visto que o novo modelo estabelece uma base para a realização de avaliações mais rigorosas e formais, tanto para finalidades internas como externas em potencial.
- Conformidade com um padrão de avaliação de processo geralmente aceito e, portanto, um forte apoio à abordagem de avaliação do processo no mercado.

Realizar Avaliações da Capacidade do Processo no COBIT 5

O padrão ISO/IEC 15504 especifica que as avaliações da capacidade do processo podem ser realizadas para diversas finalidades e com diferentes graus de rigor. Essas finalidades podem ser internas, com foco nas comparações entre as áreas da organização e/ou melhoria no processo para benefício interno, ou podem ser externas, com foco na avaliação, relatório e certificação formais.

A abordagem para a avaliação do COBIT 5 com base no ISO/IEC 15504 continua a facilitar os seguintes objetivos que têm sido a principal abordagem do COBIT desde o ano 2000:

- Permitir ao órgão de governança e à administração avaliar o desempenho da capacidade do processo.
- Permitir verificações de integridade 'do estado atual' e 'do estado desejado' em alto nível a fim de apoiar a tomada de decisão pelo órgão de governança e pela administração em relação à melhoria do processo.
- Proporcionar análises de falhas e informações para planejamento de melhorias a fim de apoiar as definições de projetos de melhorias justificáveis.
- Oferecer ao órgão de governança e à administração classificações para as avaliações a fim de medir e monitorar as capacidades atuais.

Esta seção descreve como uma avaliação em alto nível pode ser realizada com o modelo de capacidade do processo do COBIT 5 para atingir estes objetivos.

A avaliação distingue entre a capacidade de avaliação nível 1 e os níveis mais altos. De fato, conforme descrito acima, a capacidade de processo nível 1 descreve se um processo atinge os objetivos desejados e é, portanto, um nível muito importante a ser atingido - e fundamental para permitir que os níveis de capacidade mais altos sejam alcançados.

Avaliar se o processo atinge seus objetivos - ou, em outras palavras, atinge a capacidade nível 1 - pode ser feito:

1. Analisando os resultados do processo conforme a descrição detalhada de cada processo, e utilizando a escala de classificação ISO/IEC 15504 para atribuir uma classificação ao grau de consecução de cada objetivo. A escala é formada pelas seguintes avaliações:

- **N (Não atingido)** - Há pequena ou nenhuma evidência do atingimento de atributos definidos no processo avaliado. (atingimento de 0 a 15 por cento)
- **P (Parcialmente atingido)** - Há pouca evidência da abordagem e baixo atingimento do atributo definido no processo avaliado. Alguns aspectos do atingimento do atributo podem ser imprevisíveis (15 a 50 por cento de atingimento).
- **L (Amplamente atingido)** - Há evidência da abordagem sistemática e atingimento significativo do atributo definido no processo avaliado. Alguns pontos fracos referentes a este atributo podem existir no processo avaliado (50 a 85 por cento de atingimento).
- **F (Plenamente atingido)** - Há evidência da abordagem completa e sistemática e pleno atingimento do atributo definido no processo avaliado. Não existe nenhum ponto fraco significativo referente a este atributo no processo avaliado (85 a 100 por cento de atingimento).

2. Além disso, as práticas do processo (governança ou gestão) podem ser avaliadas utilizando a mesma escala de avaliação, que expressa em qual medida as práticas básicas foram aplicadas.
3. Para refinar ainda mais a avaliação, os produtos do trabalho também podem ser levados em consideração para determinar em qual medida um atributo de avaliação específico foi atingido.

Ainda que a definição dos níveis de capacidade desejados fique a critério de cada organização, muitas organizações terão a ambição de verem todos os seus processos atingirem a capacidade nível 1 (Caso contrário, qual seria o objetivo destes processos?). Se este nível não for atingido, os motivos do não atingimento deste nível ficam imediatamente evidentes a partir da abordagem explicada acima, e um plano de melhoria poderá ser definido:

1. Se o resultado do processo não for atingido de forma consistente, o processo não atingirá seu objetivo e terá de ser melhorado.
2. A avaliação das práticas do processo revelará quais práticas estão faltando ou falhando, permitindo que a implementação e/ou melhoria destas práticas seja adotada, permitindo assim que todos os resultados do processo possam ser atingidos.

Para níveis de capacidade do processo mais altos, as práticas genéricas utilizadas são extraídas do ISO/IEC 15504:2. Elas oferecem descrições genéricas para cada um dos níveis de capacidade.

ANEXO A
REFERÊNCIAS

As seguintes modelos, padrões e outras diretrizes foram utilizados como material de referência e insumo para o desenvolvimento do COBIT 5:

Association for Project Management (APM); APM Introduction to Programme Management, Latimer, Trend and Co., UK, 2007

British Standards Institute (BSI), BS25999:2007 Business Continuity Management Standard, UKUK, 2007

CIO Council, Federal Enterprise Architecture (FEA), ver 1.0, EUA, 2005

COSO

European Commission, The Commission Enterprise IT Architecture Framework (CEAF), Belgium, 2006

Kotter, John; Leading Change, Harvard Business School Press, EUA, 1996

HM Government, Best Management Practice Portfolio, Managing Successful Programmes (MSP), UKUK, 2009

HM Government, Best Management Practice Portfolio, PRINCE2®, UK, 2009

HM Government, Best Management Practice Portfolio, Information Technology Infrastructure Library (ITIL®), 2011

International Organization for Standardization (ISO), 9001:2008 Quality Management Standard, Switzeland, 2008

ISO/International Electrotechnical Commission (IEC), 20000:2006 IT Service Management Standard, Switzeland, 2006

ISO 15504

ISO/IEC, 27005:2008, Information Security Risk Management Standard, Switzeland, 2008

ISO/IEC, 38500:2008, Corporate Governance of Information Technology Standard, Switzeland, 2008

King Code of Governance Principles (King III), South Africa, 2009

Organization for Economic Co-operation and Development (OECD), OECD Principles of Corporate Governance, France, 2004

The Open Group, TOGAF® 9, UKUK, 2009

Project Management Institute, Project Management Body of Knowledge (PMBOK2®), USA, 2008

UK Financial Reporting Council, ‘Combined Code on Corporate Governance’, UK, 2009

APÊNDICE B
MAPEAMENTO DETALHADO DOS OBJETIVOS CORPORATIVOS - OBJETIVOS DE TI

A cascata de objetivos do COBIT 5 é explicado no capítulo 2.

O objetivo da tabela de mapeamento contida na figura 22 é demonstrar como os objetivos corporativos são apoiados (ou como se traduzem em) objetivos de TI. Por esse motivo, a tabela contém as seguintes informações:

- Nas colunas, todos os 17 objetivos corporativos genéricos definidos no COBIT 5, agrupados pela dimensão BSC
- Nas linhas, todos os 17 objetivos de TI, também agrupados nas dimensões BSC de TI
- Um mapeamento de como cada objetivo corporativo é apoiado pelos objetivos de TI. Este mapeamento é expresso usando a seguinte escala:
  - 'P' significa primário, quando houver uma relação importante, ou seja, quando o objetivo de TI representar um apoio fundamental para o objetivo corporativo.
  - 'S' significa secundário, quando houver uma relação ainda forte, mas menos importante, ou seja, quando o objetivo de TI representar um apoio secundário para o objetivo corporativo.

EXEMPLO 7 – TABELA DE MAPEAMENTO

A tabela de mapeamento sugere o que é normalmente esperado que:

- Objetivo Corporativo 7. Continuidade e disponibilidade do serviço de negócio:
  . Dependerá diretamente da consecução dos objetivos de TI:
    - 04 Gestão de risco organizacional de TI
    - 10 Segurança da informação, infraestrutura de processamento e aplicativos
    - 14 Disponibilidade de informações úteis e confiáveis para tomada de decisão
  . Dependerá também, mas em menor grau, da consecução dos objetivos de TI:
    - 01 Alinhamento da estratégia de TI e de negócios
    - 07 Prestação de serviços de TI em consonância com os requisitos de negócio
    - 08 Uso adequado de aplicativos, informações e soluções tecnológicas
- Usando a tabela na direção oposta, atingir o objetivo de TI 09. Agilidade de TI contribuirá para a consecução de vários objetivos corporativos:
  . Principalmente, os objetivos corporativos:
    - 2. Portfólio de produtos e serviços competitivos
    - 8. Respostas rápidas para um ambiente de negócios em mudança
    - 11. Otimização da funcionalidade do processo de negócio
    - 17. Cultura de inovação de produtos e negócios
  . Em menor grau, os objetivos corporativos:
    - 1. Valor dos investimentos da organização percebido pelas partes interessadas
    - 3. Gestão de risco organizacional (salvaguarda de ativos)
    - 6. Cultura de serviço orientada ao Cliente
    - 13. Programas de gestão de mudanças no negócio
    - 14. Produtividade operacional e da equipe
    - 16. Pessoas qualificadas e motivadas

A tabela foi criada com base nas seguintes informações:

- Pesquisas da University of Antwerp Management School IT Management e do Governance Research Institute.
- Revisões adicionais e opinião de especialistas obtidas durante o processo de desenvolvimento e revisão do COBIT 5

COBIT 5

Ao usar a tabela contida na figura 22, considerar as observações feitas no capítulo 2 sobre como usar a cascata de objetivos do COBIT 5

Figura - 22: Mapeamento dos Objetivos Corporativos do COBIT 5 em Objetivos de TI

		Objetivo Corporativo																
		Valor dos investimentos em negócio para as partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência financeira	Cultura de serviço orientada ao cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica baseada na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócio	Otimização dos custos do processo de negócio	Programa de gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com as políticas internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	Objetivo de TI	Financeira					Cliente					Interna					A&C	
Financeira	01 Alinhamento da estratégia de TI e de negócios	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 Conformidade de TI e apoio para a conformidade do negócio com as leis e regulamentos externos			S	P											P		
	03 Compromisso da gerência executiva com a tomada de decisões de TI	P	S	S					S	S		S		P			S	S
	04 Gestão do risco organizacional de TI			P	S			P	S		P			S		S	S	
	05 Benefícios obtidos pelo investimento de TI e portfólio de serviços	P	P				S		S		S	S	P		S			S
	06 Transparência dos custos, benefícios e riscos de TI	S		S		P				S	P		P					
Cliente	07 Prestação de serviços de TI em consonância com os requisitos de negócio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Uso adequado de aplicativos, informações e soluções tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09 Agilidade de TI	S	P	S			S		P			P		S	S		S	P
	10 Segurança da informação, infraestrutura de processamento e aplicativos			P	P			P								P		
	11 Otimização de ativos, recursos e capacidades de TI	P	S						S		P	S	P	S	S			S
	12 Capacitação e apoio dos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio	S	P	S			S		S		S	P	S	S	S			S
	13 Entregas de programas fornecendo benefícios, dentro do prazo, orçamento, e atendendo requisitos e padrões de qualidade	P	S	S			S				S		S	P				
	14 Disponibilidade de informações úteis e confiáveis para a tomada de decisão	S	S	S	S			P		P		S						
	15 Conformidade de TI com as políticas internas			S	S											P		
A&C	16 Equipes de TI e de negócios motivadas e qualificadas	S	S	P			S		S						P		P	S
	17 Conhecimento, expertise e iniciativas para a inovação dos negócios	S	P				S		P	S		S		S			S	P

*A&C: Aprendizado e Crescimento

APÊNDICE C
MAPEAMENTO DETALHADO DOS OBJETIVOS DE TI – PROCESSOS DE TI

Este Apêndice contém a tabela de mapeamento entre os objetivos de TI e como estes são apoiados pelos processos de TI como parte da cascata de objetivos explicada no capítulo 2.

A figura 23 contém:

- Nas colunas, todos os 17 objetivos de TI genéricos definidos no capítulo 2, agrupados nas dimensões do BSC de TI
- Nas linhas, todos os 37 processos do COBIT 5, agrupados por domínio
- Um mapeamento de como cada objetivo de TI é apoiado por um processo de TI do COBIT 5. Este mapeamento é expresso usando a seguinte escala:
  - ‘P’ significa primário, quando houver uma relação direta importante, ou seja, quando o processo do COBIT 5 for um apoio fundamental para a consecução de um objetivo de TI.
  - ‘S’ significa secundário, quando houver uma relação ainda forte, mas menos importante, ou seja, quando o processo do COBIT 5 for um apoio secundário para o objetivo de TI.
  -

EXEMPLO 8 - APO13 GERENCIAR SEGURANÇA
O Processo APO13 *Gerenciar Segurança* Contribuirá:
- Diretamente, para a consecução dos objetivos de TI:
. 02 Conformidade de TI e apoio para conformidade do negócio com leis e regulamentos externos
. 04 Gestão de risco organizacional de TI
. 06 Transparência dos custos, benefícios e riscos de TI
. 10 Segurança da informação, infraestrutura de processamento e aplicativos
. 14 Disponibilidade de informações úteis e confiáveis para tomada de decisão
- Em menor grau, para a consecução dos objetivos de TI:
. 07 Prestação de serviços de TI em consonância com os requisitos de negócio
. 08 Uso adequado de aplicativos, informações e soluções tecnológicas

A tabela foi criada com base nas seguintes informações:

- Pesquisas da University of Antwerp Management School IT Management e do Governance Research Institute.
- Revisões adicionais e opiniões de especialistas obtidos durante o processo de desenvolvimento e revisão do COBIT 5

Ao usar a tabela contida na figura 23, considerar as observações feitas no capítulo 2 sobre como usar a cascata de objetivos do COBIT 5

Figura - 23: Mapeamento dos Objetivos de TI do COBIT em Processos

			Objetivos de TI																
			Alinhamento da estratégia de TI e de negócios	Conformidade de TI e apoio para conformidade do negócio com leis e regulamentos externos	Compromisso da gerência executiva com a tomada de decisões de TI	Gestão do risco organizacional de TI	Benefícios obtidos pelo investimento de TI e portfólio de serviços	Transparência dos custos, benefícios e riscos de TI	Prestação de serviços de TI em consonância com os requisitos de negócio	Uso adequado de aplicativos, informações e soluções tecnológicas	Agilidade de TI	Segurança da informação, infraestrutura de processamento e aplicativos	Otimização de ativos, recursos e capacidades de TI	Capacitação e apoio aos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	Disponibilidade de informações úteis e confiáveis para tomada de decisão	Conformidade de TI com as políticas internas	Equipes de TI e de negócios motivadas e qualificadas	Conhecimento, expertise e iniciativas para inovação dos negócios
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processo do COBIT 5			Financeira						Cliente		Interna							A&C	
Avaliar, Dirigir e Monitorar	EDM01	Garantir a Definição e Manutenção do Modelo de Governança	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Garantir a Realização de Benefícios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Garantir a Otimização do Risco	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Garantir a Otimização de Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Garantir a Transparência às Partes Interessadas	S	S	P			P	P						S	S	S		S
Alinhar, Planejar e Organizar	APO01	Gerenciar a Estrutura de Gestão de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gerenciar a Estratégia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gerenciar Arquitetura da Organização	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gerenciar Inovação	S			S	P			P	P		P	S		S			P
	APO05	Gerenciar Portfólio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gerenciar Orçamento e Custos	S		S	S	P	P	S	S			S		S				
	APO07	Gerenciar Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gerenciar Relacionamentos	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gerenciar Contratos de Prestação de Serviços	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gerenciar Fornecedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gerenciar Qualidade	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gerenciar Riscos		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gerenciar Segurança		P		P		P	S	S		P				P			

Figure - 23: Mapeamento dos Objetivos de TI do COBIT em Processos

			Objetivos de TI																
			Alinhamento da estratégia de TI e de negócios	Conformidade de TI e apoio para conformidade do negócio com leis e regulamentos externos	Compromisso da gerência executiva com a tomada de decisões de TI	Gestão do risco organizacional de TI	Benefícios obtidos pelo investimento de TI e portfólio de serviços	Transparência dos custos, benefícios e riscos de TI	Prestação de serviços de TI em consonância com os requisitos de negócio	Uso adequado de aplicativos, informações e soluções tecnológicas	Agilidade de TI	Segurança da informação, infraestrutura de processamento e aplicativos	Otimização de ativos, recursos e capacidades de TI	Capacitação e apoio aos processos de negócio através da integração de aplicativos e tecnologia nos processos de negócio	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos e padrões de qualidade	Disponibilidade de informações úteis e confiáveis para tomada de decisão	Conformidade de TI com as políticas internas	Equipes de TI e de negócios motivadas e	Conhecimento, expertise e iniciativas para inovação dos negócios
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processo do COBIT 5			Financeira						Cliente		Interna							A&D	
Construir, Adquirir e Implementar	BAI01	Gerenciar Programas e Projetos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gerenciar Definição de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gerenciar Identificação e	S			S	S		P	S			S	S	S	S			S
	BAI04	Gerenciar Disponibilidade e				S	S		P	S	S		P		S	P			S
	BAI05	Gerenciar Capacidade de Mudança	S		S		S		S	P	S		S	S	P				P
	BAI06	Gerenciar Mudanças			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gerenciar Aceitação e Transição da Mudança				S	S		S	P	S			P	S	S	S		S
	BAI08	Gerenciar	S				S		S	S	P	S	S			S		S	P
	BAI09	Gerenciar Ativos		S		S		P	S		S	S	P			S	S		
	BAI10	Gerenciar Configuração		P		S		S		S	S	S	P			P	S		
Entregar, Atender e Apoiar	DSS01	Gerenciar Operações		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gerenciar Solicitações e Incidentes de Serviços				P			P	S		S				S	S		S
	DSS03	Gerenciar Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gerenciar Continuidade	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gerenciar Serviços de Segurança	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gerenciar Controles do Processo de Negócio		S		P			P	S		S	S	S		S	S	S	S
Monitorar, Avaliar e Analisar	MEA01	Monitorar, Avaliar e Analisar Desempenho e Conformidade	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitorar, Avaliar e Analisar o Sistema de Controle Interno		P		P		S	S	S		S				S	P		S
	MEA03	Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos		P		P	S		S			S					S		S

*A&C: Aprendizado e Crescimento

APÊNDICE D
NECESSIDADES DAS PARTES INTERESSADAS E OBJETIVOS CORPORATIVOS

O Capítulo 4 ilustrou as etapas individuais da navegação pela cascata de objetivos, desde as necessidades das partes interessadas até as metas dos habilitadores.

O Capítulo 2 incluiu uma tabela com perguntas comuns sobre governança e gestão de TI. Do ponto de vista das partes interessadas, é importante saber como estas perguntas se relacionam com os objetivos corporativos. Por este motivo, a figura 24 foi incluída; ela mostra como uma lista de necessidades da de uma parte interessada interna à organização pode ser associada aos objetivos corporativos.

Esta tabela pode ser usada para ajudar a definir e priorizar objetivos corporativos ou objetivos de TI específicos, com base nas necessidades especificas das partes interessadas. As mesmas precauções devem ser tomadas ao usar estas tabelas, assim como com as demais tabelas da cascata de objetivos, ou seja, a situação de cada organização é diferente, de modo que estas tabelas não devem ser usadas de forma mecânica, mas somente como uma sugestão de um conjunto de relacionamentos genéricos. Na figura 24, a intersecção da necessidade de uma parte interessada com o objetivo corporativo é preenchida se aquela necessidade tiver de ser considerada para aquele objetivo.

Figura – 24: Mapeamento dos Objetivos Corporativos do COBIT 5 em Perguntas sobre Governança e Gestão

Necessidades das partes interessadas	Valor dos investimentos da organização percebido pelas partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência Financeira	Cultura de serviço orientada ao Cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica com base na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócios	Otimização dos custos do processo de negócios	Programas De gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com Políticas Internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Como faço para obter valor com o uso de TI? Os usuários finais estão satisfeitos com a qualidade do serviço de TI?	■	■				■	■						■			■	■
Como posso gerenciar o desempenho de TI?		■			■				■	■	■	■		■			
Como posso explorar melhor as novas tecnologias para novas oportunidades estratégicas?	■	■						■					■			■	■
Como faço para criar e estruturar da melhor forma o meu departamento de TI?								■		■	■	■		■	■	■	
Qual é a minha dependência de fornecedores externos? Quão bem os contratos de terceirização de TI estão sendo gerenciados? Como faço para obter garantia dos fornecedores externos?			■	■						■							

Figura – 24: Mapeamento dos Objetivos Corporativos do COBIT 5 em Perguntas sobre Governança e Gestão																	
Necessidades das partes interessadas	Valor dos investimentos da organização percebido pelas partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência Financeira	Cultura de serviço orientada ao Cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica com base na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócios	Otimização dos custos do processo de negócios	Programas De gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com Políticas Internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Quais são os requisitos (de controle) da informação?				■					■						■		
Considerei todos os riscos de TI?			■				■		■						■		
Estou conduzindo uma resiliente e eficiente operação de TI?					■		■										
Como posso controlar o custo de TI? Como utilizar os recursos de TI de forma mais eficaz e eficiente? Quais são as opções de terceirização mais efetivas e eficientes?										■		■		■			
Tenho pessoal suficiente para TI? Como faço para desenvolver e manter sua capacitação, e como controlo seu desempenho?										■		■		■			
Como faço para obter garantia do funcionamento de TI?				■											■		
As informações que estou processando estão bem protegidas?				■			■								■		
Como posso melhorar a agilidade dos negócios com um ambiente de TI mais flexível?	■							■								■	■
Os projetos de TI falham para entregar o que prometeram – e caso afirmativo, por quê? TI está atrapalhando a execução da estratégia de negócios?	■	■	■					■			■	■	■				
Quão crítica é TI para a sustentação da organização? O que fazer se ela não estiver disponível?	■	■					■										
Quais processos de negócios críticos dependem de TI, e quais são os requisitos dos processos de negócios?	■	■									■	■					

Figura – 24: Mapeamento dos Objetivos Corporativos do COBIT 5 em Perguntas sobre Governança e Gestão

Necessidades das partes interessadas	Valor dos investimentos da organização percebido pelas partes interessadas	Portfólio de produtos e serviços competitivos	Gestão de risco organizacional (salvaguarda de ativos)	Conformidade com as leis e regulamentos externos	Transparência Financeira	Cultura de serviço orientada ao Cliente	Continuidade e disponibilidade do serviço de negócio	Respostas rápidas para um ambiente de negócios em mudança	Tomada de decisão estratégica com base na informação	Otimização dos custos de prestação de serviços	Otimização da funcionalidade do processo de negócios	Otimização dos custos do processo de negócios	Programas De gestão de mudanças no negócio	Produtividade operacional e da equipe	Conformidade com Políticas Internas	Pessoas qualificadas e motivadas	Cultura de inovação de produtos e negócios
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Qual tem sido o custo adicional médio dos orçamentos operacionais de TI? Com que frequência e em que medida os projetos de TI estouram o orçamento?					■					■		■		■			
Quanto do esforço de TI é dedicado para apagar incêndios em vez de facilitar a melhoria do negócio?		■	■									■					
Foram disponibilizados infraestruturas e recursos de TI suficientes para alcançar os objetivos estratégicos da organização?		■			■					■		■					
Quanto tempo é necessário para a tomada de decisões importantes de TI?	■	■			■			■									
O esforço total de TI e seus investimentos são transparentes?		■		■	■										■		
A TI apoia a organização no cumprimento dos regulamentos e níveis de serviço? Como faço para saber se estou em conformidade com todos os regulamentos aplicáveis?				■											■		

APÊNDICE E
MAPEAMENTO DO COBIT 5 COM OS PADRÕES E MODELOS CORRELATOS MAIS RELEVANTES

Introdução

Este Apêndice compara o COBIT 5 com os padrões e modelos mais relevantes e utilizados no âmbito da governança. Para a ISO/IEC 38500 (ABNT NBR ISO/IEC 38500) isto é feito por meio de uma comparação baseada nos princípios do ISO/IEC 38500; para as demais comparações foi utilizada uma tabela em que os processos do COBIT 5 são mapeados contra os conteúdos equivalentes no referido padrão ou modelo.

COBIT 5 e ISO/IEC 38500

A seguir é resumida a forma como o COBIT 5 apoia a adoção dos princípios e abordagem de implementação do padrão. O padrão ISO/IEC 38500:2008 – Governança corporativa da tecnologia da informação – baseia-se em seis princípios básicos. As implicações práticas de cada princípio são explicadas aqui, juntamente com a forma como as orientações do viabilizam sua boa prática.

Princípios do ISO/IEC 38500

1º PRINCÍPIO - RESPONSABILIDADE

O que isso significa na prática:

A organização (cliente) e TI (fornecedor) deverão colaborar em um modelo de parceria utilizando comunicações efetivas baseadas um relacionamento positivo e confiável e demostrando clareza em relação às responsabilidades. Para organizações de maior porte, um comitê executivo de TI (também denominado comitê estratégico de TI) atuando em nome do conselho e presidido por um membro do conselho é um mecanismo muito efetivo para avaliar, orientar e monitorar o uso de TI na organização e para orientar o conselho em relação às questões críticas de TI. Diretores de organizações de pequeno e médio portes, com uma estrutura de comando mais simples e fluxos de comunicação mais rápidos, devem adotar uma abordagem mais direta ao supervisionar as atividades de TI. Em todos os casos, as estruturas, funções e responsabilidades adequadas de governança corporativa devem ser definidas pelo corpo diretivo, demonstrando clara propriedade e responsabilização com relação a decisões e tarefas importantes. Isso deverá incluir o relacionamento com os principais prestadores de serviços de TI terceirizados.

Como a orientação da ISACA viabiliza a boa prática:

1. O modelo do COBIT 5 define uma série de habilitadores para governança corporativa de TI. O habilitador “processo” e o habilitador “estruturas organizacionais”, combinados com asas tabelas RACI[13] são especialmente pertinentes nesse contexto. Eles reforçam a atribuição de responsabilidades, e fornecem exemplos de funções e responsabilidades para os membros do conselho e administradores para todos os principais processos e atividades correlatas.
2. O COBIT 5 Implementação explica as responsabilidades das partes interessadas e demais envolvidos na implementação ou aperfeiçoamento dos arranjos de governança de TI.
3. O COBIT 5 possui dois níveis de monitoramento. O primeiro nível é pertinente a um contexto de governança. O processo EDM05 Garantir transparência às partes interessadas explica a função do diretor no monitoramento e avaliação da governança e do desempenho dada TI com um método genérico para estabelecer metas e objetivos bem como os indicadores relacionados.

2º PRINCÍPIO - ESTRATÉGIA

O que isso significa na prática:

O planejamento estratégico de TI é um empreendimento complexo e crítico, que exige uma estreita coordenação com as unidades de negócios da organização. É também vital priorizar os planos com maior probabilidade de alcançar os benefícios desejados e para alocar os recursos dede maneira efetiva. Objetivos de alto nível devem ser traduzidos em planos táticos executáveis, que minimizem falhas e surpresas. O objetivo é gerar valor apoiando os objetivos estratégicos e considerando os riscos associados em relação ao apetite de risco dada alta administração. Embora seja importante desdobrar os planos de cima para baixo, os planos também deverão ser flexíveis e adaptáveis para atender às rápidas mudanças nos requisitos de negócios e às oportunidades em TI.

Além disso, a presença ou ausência das capacidades de TI podem viabilizar ou dificultar as estratégias de negócios. Portanto. Portanto, o planejamento estratégico de TI deverá incluir um planejamento adequado e transparente das capacidades de TI. Esse planejamento deverá incluir uma avaliação da capacidade da atual estrutura de TI e dos recursos humanos para apoiar futuros requisitos do negócio e levar em consideração futuros desenvolvimentos tecnológicos que possam permitir uma vantagem competitiva e/ou otimização de custos. Recursos de TI incluem parcerias com diversos fornecedores de produtos e prestadores de serviços externos, alguns dos quais provavelmente exercem uma função crítica na sustentação do negócio. A governança do fornecimento estratégico é, portanto, uma atividade de planejamento estratégico significativa, que exige a orientação e supervisão em nível executivo.

[13] Matriz RACI define o Responsável, Aprovador, Consultado e Informado em relação a uma tarefa.

Como a orientação da ISACA viabiliza a boa prática:

1. O COBIT 5 fornece orientação específica sobre a gestão de investimentos em TI e (especialmente, no processo *EDM02 Garantir a realização de benefícios* no domínio de governança) como os objetivos estratégicos devem ser apoiados por estudos de casos (business cases) adequados.
2. O domínio APO do COBIT 5 explica os processos necessários para o planejamento e organização efetivos dos recursos internos e externos de TI, incluindo o planejamento estratégico, planejamento tecnológico e arquitetural, planejamento organizacional, planejamento de inovação, gestão do portfólio, gestão de investimentos, gestão de riscos, gestão de gestão de relacionamentos e gestão de qualidade. O alinhamento dos objetivos dede negócio e de TI também é explicado, com exemplos genéricos que mostram como eles auxiliam os objetivos estratégicos de todos os processos de TI com base em amplas pesquisas.
3. O exercício de identificar e alinhar os objetivos corporativos e os objetivos de TI apresenta um melhor entendimento da relação de desdobramento dos objetivos corporativos, os objetivos de TI e os habilitadores, o que inclui os processos de TI. É apresentada uma sólida e consistente lista de 17 objetivos corporativos genéricos e 17 objetivos de TI genéricos, validados e priorizados entre diferentes setores. Juntamente com as informações vinculadas entre ambos, isso fornece uma boa base sobre a qual será construída a cascata genérica de objetivos corporativos em objetivos de TI.

3º PRINCÍPIO - AQUISIÇÃO

O que isso significa na prática:

Soluções de TI existem para apoiar os processos de negócios e, portanto, deve-se tomar cuidado para não considerar as soluções de TI isoladamente ou apenas como um projeto ou serviço de “tecnologia”. Por outro lado, uma escolha inadequada de arquitetura tecnológica, uma falha em manter uma infraestrutura técnica atualizada e adequada ou a falta de recursos humanos capacitados pode resultar em falhas de projeto, na incapacidade de sustentar as operações da organização ou na redução no valor do negócio. As aquisições de recursos de TI deverão ser consideradas como parte de uma ampla mudança nono negócio habilitada por TI. A tecnologia adquirida também deverá apoiar e operar com os processos de negócios e infraestruturas de TI existentes e planejados. A implementação também não é apenas uma questão de tecnologia, mas sim uma combinação de mudança organizacional, revisão dos processos de negócios, treinamento e viabilização da mudança. Portanto, os projetos de TI devem ser considerados como parte de programas mais amplos de mudança corporativa que incluem outros projetos, contemplando todas as atividades necessárias a assegurar um resultado positivo.

Como a orientação da ISACA viabiliza a boa prática:

1. O domínio EDM do COBIT 5 fornece orientação sobre como governar e gerenciar os investimentos de negócio habilitados por TI através de todo seu ciclo de vida completo (aquisição, implementação, (aquisição, implementação, operação e descarte). O processo APO05 Gerenciar o portfólio aborda como aplicar com eficiência a gestão de portfólio e programas a tais investimentos para ajudar a garantir que os benefícios sejam realizados e os custos otimizados.
2. O domínio APO do COBIT 5 fornece orientação para o planejamento de aquisição, inclusive planejamento de investimentos, gestão de riscos, planejamento de programas e projetos bem como planejamento da qualidade.
3. O domínio BAI do COBIT 5 fornece orientação sobre os processos necessários para adquirir e implementar soluções de TI, cobrindo a definição de requisitos, identificação de soluções viáveis, preparação da documentação e treinamento e capacitação dos usuários e operações para execução nos novos sistemas. Além disso, é fornecida orientação para assegurar que as soluções sejam testadas e controladas adequadamente conforme a mudança for aplicada à operação do negócio da organização e ao ambiente de TI.
4. O domínio MEA do COBIT 5 e o processo EDM05 incluem orientação sobre como a diretoria pode monitorar o processo de aquisição e controles internos para assegurar que as aquisições sejam gerenciadas e executadas adequadamente.

4º PRINCÍPIO - DESEMPENHO

O que isso significa na prática:

A medição efetiva do desempenho depende de dois aspectos principais: a definição clara das metas de desempenho e o estabelecimento de Indicadores efetivas para monitorar o atingimento dos objetivos. Um processo de medição de desempenho também é necessário para assegurar que o desempenho seja monitorado de forma consistente e confiável. A governança efetiva é atingida quando os objetivos são determinados de cima para baixo, alinhados com os objetivos corporativos de alto nível aprovados, e os Indicadores são estabelecidas de baixo para cima, alinhadas de forma que permitam que o atingimento dos objetivos seja monitorado em todos os níveis por cada camada da gestão. Dois fatores críticos de sucesso da governança são a aprovação dos objetivos pelas Partes Interessadas, e a aceitação da responsabilidade pelo atingimento dos objetivos pelos diretores e gerentes. TI é um tema complexo e técnico, entretanto é importante alcançar transparência expressando os objetivos, os indicadores e os relatórios de desempenho em uma linguagem que possa ser entendida pelas Partes Interessadas, permitindo com que medidas apropriadas possam ser tomadas.

Como a orientação da ISACA viabiliza a boa pratica:

1. O modelo do COBIT 5 fornece exemplos genéricos de metas e indicadores para todos os processos de TI e demais habilitadores, e mostra como eles se relacionam com os objetivos do negócio, permitindo sua adaptação pelas organizações para sua aplicação específica.
2. O COBIT 5 fornece à gestão orientação sobre a definição dos objetivos de TI em consonância com os objetivos do negócio e descreve como monitorar o desempenho destes objetivos com a utilização de metas e indicadores. A capacidade do processo pode ser avaliada com o uso do modelo de avaliação de capacidade previsto na norma ISO/IEC 15504
3. Dois processos chave do COBIT 5 fornecem orientação específica:
   - APO02 Gerenciar a estratégia, que concentra-se na definição de objetivos.

- APO09 Gerenciar contratos de prestação de serviços, que concentra-se na definição dos serviços adequados e objetivos do serviço bem como documenta-los por meio de acordos de nível de serviço.

4. No processo MEA01 Monitorar, avaliar e analisar o desempenho e a conformidade, o COBIT 5 fornece orientação sobre as responsabilidades da gestão executiva para esta atividade.
5. O guia COBIT 5 para Avaliação explicará como os profissionais de avaliação podem fornecer garantia independente à diretoria em relação ao desempenho de TI.

5º PRINCÍPIO - CONFORMIDADE

O que isso significa na prática:

No mercado global atual, capacitado pela Internet e tecnologias avançadas, as organizações precisam cumprir um crescente número de exigências legais e regulatórias. Devido a escândalos corporativos e a crises financeiras nos últimos anos, há uma maior conscientização dos membros da alta administração da existência e implicações de leis e regulamentos mais rigorosos. As partes interessadas exigem uma maior garantia de que as organizações estejam atuando conforme as leis e regulamentos e em conformidade com boas práticas de governança corporativa em seu ambiente dede atuação. Além disso, devido ao fato de a TI ter permitido processos de negócios pervasivos integrados entre organizações, há ainda uma crescente necessidade de assegurar que os contratos incluam importantes requisitos de TI em áreas tais como privacidade, confidencialidade, propriedade intelectual e segurança.

A diretoria deve garantir que o cumprimento dos regulamentos externos seja tratado como parte de um planejamento estratégico ao invés de somente se materializar em uma reação tardia e custosa. Os membros da alta direção também devem dar o tom do alto escalão e estabelecer políticas e procedimentos para seus gerentes e equipes, visando garantir que os objetivos corporativos sejam alcançados, o risco seja minimizado e a conformidade seja atingida. AA alta gerência deverá encontrar o equilíbrio adequado entre desempenho e conformidade, garantindo que as metas de desempenho não coloquem em risco a conformidade e, de forma recíproca, que o regime de conformidade seja adequado e não restrinja excessivamente a operação do negócio.

Como a orientação da ISACA viabiliza a boa pratica:

1. As práticas de governança e gestão do COBIT 5 fornecem uma base para o estabelecimento de um ambiente de controle adequado na organização. As avaliações de capacidade de processo permitem que a administração avalie e compare o desempenho e a capacidade dos processos de TI.
2. 2. O processo do COBIT 5 APO02 Gerenciar a estratégia ajuda a garantir a existência de um alinhamento entre o plano de TI e os objetivos gerais da organização, inclusive as exigências de governança.
3. 3. O processo do COBIT 5 MEA02 Monitorar, avaliar e analisar o sistema de controle interno permite que a diretoria avalie se os controles são adequados para cumprir os requisitos de conformidade.
4. 4. O processo do COBIT 5 MEA03 Monitorar, avaliar e analisar a conformidade com os requisitos externos ajuda a garantir que os requisitos de conformidade externos sejam identificados, a alta direção estabeleça a orientação para a conformidade e a conformidade de TI em si seja monitorada, avaliada e informada como parte da conformidade geral com os requisitos da organização.
5. O guia COBIT 5 **para Avaliação** explica como os auditores podem fornecer uma garantia independente da conformidade e aderência às políticas derivadas de diretivas internas ou de exigências legais, regulatórias ou contratuais externas, confirmando que todas as ações corretivas para tratar de qualquer falha na conformidade tenham sido tomadas tempestivamente pelo responsável pelo processo.

6º PRINCÍPIO - COMPORTAMENTO HUMANO

O que isso significa na prática:

A implementação de qualquer mudança habilitada por TI, inclusive na governança de TI em si, geralmente exige uma mudança cultural e comportamental significativa das organizações e na relação com seus clientes e parceiros comerciais. Isso pode causar medo e mal-entendido entre as equipes, de modo que a implementação deve ser administrada cuidadosamente a fim de manter o pessoal positivamente engajado. A alta direção deverá comunicar claramente os objetivos e ser percebidos como apoiando positivamente as mudanças propostas. Treinamento e capacitação dos funcionários são aspectos chave da mudança — especialmente em função da natureza de mudança rápida da tecnologia. Pessoas são afetadas pela TI em todos os níveis dada organização, como as partes interessadas, gestores e usuários, ou especialistas que prestam serviços e soluções de TI para a organização. Além da organização, a TI afeta clientes e parceiros comerciais e permite cada vez mais o auto atendimento em serviços de TI e as transações automatizadas entre organizações em nível doméstico e internacional. Enquanto os processos de negócios habilitados por TI trazem novos benefícios e oportunidades, eles também ampliam os tipos de riscos. O interesse das pessoas por questões sobre privacidade e fraudes está aumentando, e estes e os demais tipos de riscos devem ser geridos para que as pessoas tenham confiança nos sistemas de TI que utilizam. Sistemas de informação também podem afetar drasticamente os métodos de trabalho por meio da automação dos procedimentos manuais.

Como a orientação da ISACA viabiliza a boa prática:

Os seguintes habilitadores do COBIT 5 (inclusive processos) fornecem orientação sobre as exigências relativas ao comportamento humano:

1. Os habilitadores do COBIT 5 incluem pessoas, habilidades e competências, bem como cultura, ética e comportamento. Para cada habilitador é apresentado um modelo de como se deve lidar com este habilitador, ilustrado com exemplos.
2. O processo do COBIT 5 APO07 Gerenciar recursos humanos explica como o desempenho dos indivíduos deve ser alinhado aos objetivos corporativos, como as habilidades dos especialistas em TI devem ser mantidas, e como e responsabilidades devem ser definidas.

3. O processo do COBIT 5 BAI02 Gerenciar definição de requisitos ajuda a assegurar que o projeto dos aplicativos atenda às exigências de uso e operação por pessoas.
4. Os processos do COBIT 5 BAI05 Gerenciar capacidade de mudança organizacional e BAI08 Gerenciar conhecimento ajuda a garantir que os usuários estejam habilitados para utilizar os sistemas dede modo efetivo.
5. Além disso, a ISACA fornece quatro certificações para profissionais que desempenham funções chave relacionadas à governança de TI, e para as quais a base do conhecimento é substancialmente coberta pelos conteúdos pelo conteúdo do COBIT 5

- Certificado de Governança Corporativa de TI ® (CGEIT®)
- Certificado de Auditor de Sistemas de Informação ® (CISA®)
- Certificado de Gerente de Segurança da Informação ® (CISM®)
- Certificado de Controle de Riscos e Sistemas de Informação (CRISC®)

Os detentores destes certificados demonstram, tanto capacidade, quanto experiência no desempenho dessas funções.

ISO/IEC 38500 Avaliar, Dirigir e Monitorar a ISO/IEC 38500

Como a orientação da ISACA viabiliza a boa prática:

O domínio de governança no modelo de processo do COBIT 5 possui cinco processos e cada um destes processos possui práticas de avaliação, direção e monitoramento (EDM) definidas. Este é o principal local no COBIT 5 onde atividades de governança são definidas.

Comparação com Outros Padrões

O COBIT 5 foi desenvolvido considerando uma série de outros padrões e modelos de referência. Estes. Esses padrões estão relacionados no Apêndice A.

O COBIT 5: Habilitador Processos contém um mapeamento em alto nível entre cada processo do COBIT 5 e as partes mais importantes dos respectivos padrões e modelos onde podem ser obtidas orientações adicionais.

Esta seção inclui uma breve discussão sobre cada modelo ou padrão, indicando a quais áreas e domínios do COBIT 5 ela se refere.

ITIL® e ISO/IEC 20000 (ABNT NBR ISO/IEC 20000)

As seguintes áreas e domínios do COBIT 5 são cobertas pelo ITIL e ISO/IEC 20000:

- Um subconjunto de processos do domínio DSS
- Um subconjunto de processos do domínio BAI
- Alguns processos do domínio APO

ISO/IEC Série 27000 (ABNT NBR ISO/IEC 27000)

As seguintes áreas e domínios do COBIT 5 são cobertas pelo ISO/IEC 27000:

- Processos relativos à segurança e riscos dos domínios EDM, APO e DSS
- Diversas atividades de segurança dentro dos processos em outros domínios
- Atividades de monitoramento e avaliação a partir do domínio MEA

ISO/IEC Série 31000 (ABNT NBR ISO 31000)

As seguintes áreas e domínios do COBIT 5 são cobertas pelo ISO/IEC 31000:

- Processos de gestão de risco dos domínios EDM e APO

TOGAF®

As seguintes áreas e domínios do COBIT 5 são cobertas pelo TOGAF:

- Processos relacionados a recursos no domínio EDM (governança) – Os componentes do TOGAF dos Modelos de Maturidade de Arquitetura, Governança de Arquitetura e Conselho de Arquitetura relacionam-se com otimização dos recursos.
- O processo de arquitetura corporativa no domínio APO. No núcleo do TOGAF está o ciclo do Método de Desenvolvimento de Arquitetura (ADM), que mapeia para o COBIT 5 as práticas de desenvolvimento de uma visão de arquitetura (ADM Fase A), definição de arquiteturas de referência (ADM Fases B, C, D), seleção de oportunidades e soluções (ADM Fase E) e definição da implementação da arquitetura (ADM Fases F, G). Diversos componentes do TOGAF apontam para a prática do COBIT 5 de provimento de serviços de arquitetura empresarial. Isso inclui:
  - Gestão de Requisitos de ADM
  - Princípios da Arquitetura
  - Gestão de Partes interessadas
  - Avaliação da Aptidão para Mudança Corporativa
  - Gestão de Riscos
  - Planejamento com Base na Capacidade
  - Conformidade da Arquitetura
  - Contratos de Arquitetura

Capability Maturity Model Integration (CMMI) (desenvolvimento)

As seguintes áreas e domínios do COBIT 5 são cobertas pelo CMMI:

- Processos relativos à aquisição e desenvolvimento de aplicativos do domínio BAI
- Alguns processos organizacionais e relacionados à qualidade a partir do domínio APO

PRINCE2®

As seguintes áreas e domínios do COBIT 5 são cobertas pelo PRINCE2:

- Processos relativos ao portfólio no domínio APO
- Processos de gestão de projetos e programas no domínio BAI

A **figura 25** ilustra a relação de cobertura entre o COBIT 5 e os demais padrões e modelos.

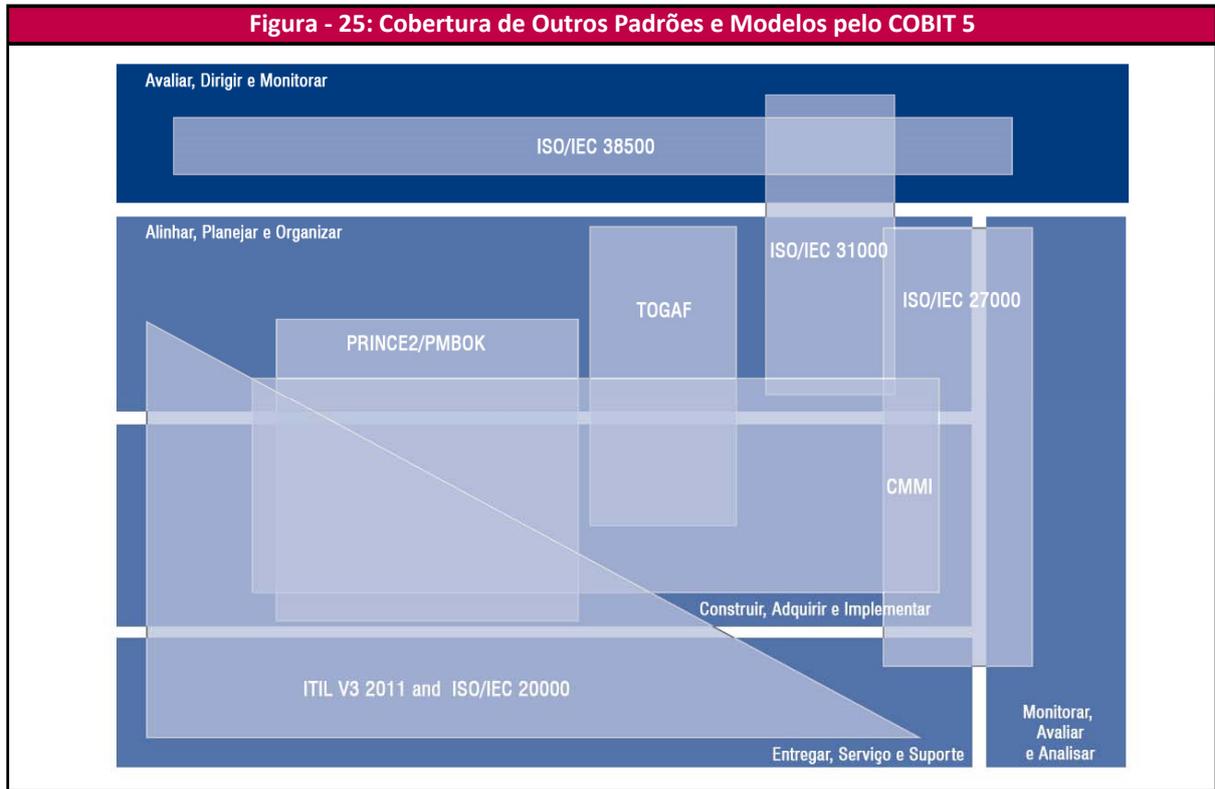



Figura - 25: Cobertura de Outros Padrões e Modelos pelo COBIT 5

APÊNDICE F
COMPARAÇÃO ENTRE O MODELO DE INFORMAÇÕES DO COBIT 5 E OS CRITÉRIOS DE INFORMAÇÕES DO COBIT 4.1

Como os sete critérios de avaliação do COBIT 4.1 - eficácia, eficiência, integridade, confiabilidade, disponibilidade, confidencialidade e conformidade - se relacionam com as categorias de qualidade da informação e as dimensões dos habilitadores informação do COBIT 5, conforme demonstrado no Apêndice G, figura 32

A tabela abaixo possui duas colunas:

- A primeira coluna relaciona cada um dos sete critérios de informações do COBIT 4.1.
- A segunda coluna relaciona as alternativas do COBIT 5, ou seja, a(s) respectiva(s) meta(s) do habilitador informação.

Figura - 26: Equivalentes do COBIT 5 aos Critérios de Informação do COBIT 4.1

Critérios de Informação COBIT 4.1	Equivalente do COBIT 5
Eficácia	A informação é eficaz se atender às necessidades do consumidor da informação que a utiliza para uma tarefa específica. Se o consumidor da informação puder realizar a tarefa com a informação, então a informação é eficaz. Isso corresponde às seguintes metas de qualidade da informação: valor adequado, relevância, compreensibilidade, interpretabilidade e objetividade.
Eficiência	Considerando que a eficácia leva em conta a informação como um produto, a eficiência se refere mais ao processo de obtenção e uso da informação, assim ela se alinha à visão de "informação como um serviço". Se a informação que atende às necessidades do consumidor da informação for obtida e usada facilmente (por exemplo, necessitar de poucos recursos – esforço físico, esforço cognitivos, tempo e dinheiro), então o uso da informação será considerado eficiente. Isso corresponde às seguintes metas de qualidade da informação: credibilidade, acessibilidade, facilidade de operação e reputação.
Integridade	Se a informação tiver integridade, então ela será exata e completa. Isso corresponde às seguintes metas de qualidade da informação: completude e exatidão.
Confiabilidade	A confiabilidade é frequentemente vista como sinônimo de exatidão; no entanto, também se pode dizer que a informação é confiável se ela for considerada verdadeira e confiável. Comparada com a integridade, a confiabilidade é mais subjetiva, mais relacionada à percepção, e não somente aos fatos. Ela corresponde às seguintes metas de qualidade da informação: credibilidade, reputação e objetividade.
Disponibilidade	A disponibilidade é uma das metas de qualidade da informação sob a orientação da acessibilidade e segurança.
Confidencialidade	A confidencialidade corresponde às metas de qualidade da informação no que diz respeito à restrição ao acesso.
Conformidade	A conformidade no sentido de que a informação deve cumprir as especificações é coberta por qualquer uma das metas de qualidade da informação, dependendo dos seus requisitos.

Esta tabela mostra que todos os critérios de informações do COBIT 4.1 são cobertos pelo COBIT 5; no entanto, o modelo de informações do COBIT 5 permite a definição de uma configuração adicional de critérios, consequentemente agregando valor aos critérios do COBIT 4.1.

APÊNDICE G
DESCRIÇÃO DETALHADA DOS HABILITADORES DO COBIT 5

Introdução

Esta seção discute com mais detalhes as sete categorias de habilitadores que fazem parte do modelo do COBIT 5 que inicialmente, foram descritas no capítulo 5 e são reapresentados na figura 27.

Figura - 27: Habilitadores do COBIT 5: Genéricos

Dimensão do Habilitador
Partes Interessadas
• Partes Interessadas Internas
• Partes Interessadas Externas
Objetivos
• Qualidade Intrínseca
• Qualidade Contextual (relevância, eficácia)
• Assessibilidade e Segurança
Ciclo de Vida
• Planejar
• Projetar
• Desenvolver / Adquirir / Criar / Implementar
• Usar/Operar
• Avaliar / Monitorar
• Atualizar / Descartar
Boas Práticas
• Práticas
• Produtos do trabalho (Entradas/Saídas)
Controle do Desempenho do Habilitador
As necessidades das partes interessadas foram atendidas?
As metas do habilitador foram atingidas?
O Ciclo de Vida é Gerenciado?
Boas Práticas Foram Aplicadas?
Indicadores para Atingimento das Metas (Indicadores de Resultado)
Indicadores para Aplicação das Práticas (Indicadores de Desempenho ou Execução)

Dimensões do Habilitador

As quatro dimensões comuns dos habilitadores são:

- **Partes Interessadas** - Cada habilitador tem partes interessadas (partes que desempenham um papel ativo e/ou tenham algum interesse no habilitador). Por exemplo, os processos têm diversas partes que executam atividades do processo e/ou que tenham algum interesse nos resultados do processo; estruturas organizacionais têm interessados, cada um com suas próprias funções e interesses que fazem parte dos modelos. As Partes interessadas podem ser internas ou externas à organização, e todos possuem seus próprios, e às vezes conflitantes, interesses e necessidades. As necessidades das partes interessadas são traduzidas em objetivos corporativos, que por sua vez são traduzidos em objetivos corporativos de TI. Uma lista de partes interessadas é apresentada na figura 7.
- **Metas** - Cada habilitador tem diversas metas, e os habilitadores criam valor através do atingimento dessas metas. Metas podem ser definidas em termos de:
  - Resultados esperados do habilitador
  - Aplicação ou operação do próprio habilitador

    As metas do habilitador são a última etapa da cascata de objetivos do COBIT 5. Essas metas podem ser divididas ainda em diferentes categorias:
  - **Qualidade intrínseca** - Em que medida os habilitadores trabalham de forma precisa, objetiva e produzem resultados exatos, objetivos e confiáveis
  - **Qualidade contextual** - Em que medida os habilitadores e seus resultados cumprem suas metas levando-se em consideração o contexto em que operam. Por exemplo, os resultados devem ser pertinentes, completos, atuais, apropriados, consistentes, compreensíveis e fáceis de usar.
  - **Acesso e segurança** - Em que medida os habilitadores e seus resultados são acessíveis e seguros, tais como:
    - Os habilitadores estão disponíveis quando, e se, necessário.
    - Os resultados são seguros, ou seja, o acesso é restrito a quem de direito e que precisar deles.
- **Ciclo de vida** - Cada habilitador tem um ciclo de vida, desde sua criação, passando por sua vida útil/operacional até chegar ao descarte. Isto se aplica às informações, modelos, processos, políticas, etc. As fases do ciclo de vida incluem:
  - Planejar (inclui o desenvolvimento e seleção de conceitos)
  - Projetar
  - Desenvolver/adquirir/criar/implementar
  - Usar/operar
  - Avaliar/monitorar

– Atualizar/descartar

- **Boas práticas** - Boas práticas podem ser definidas para cada um dos habilitadores. Boas práticas apoiam o atingimento das metas do habilitador. Boas práticas oferecem exemplos ou sugestões de como implementar o habilitador da melhor maneira, e quais produtos do trabalho ou entradas e saídas são necessários. O COBIT 5 oferece exemplos de boas práticas para alguns dos habilitadores do COBIT 5 (ex: processos). Para outros habilitadores pode-se usar a orientação dos demais padrões, modelos, etc.

Controle de Desempenho do Habilitador

Organizações esperam resultados positivos da aplicação e uso dos habilitadores. Para controlar o desempenho dos habilitadores, as perguntas abaixo terão de ser monitoradas e posteriormente respondidas - com base em indicadores - periodicamente:

- As necessidades das partes interessadas foram consideradas?
- As metas do habilitador foram atingidas?
- O ciclo de vida do habilitador é controlado?
- Boas práticas foram aplicadas?

Os dois primeiros marcadores tratam do resultado efetivo do habilitador. Os indicadores usados para aferir em que medida as metas foram atingidas podem ser chamadas de 'indicadores de resultado'.

Os dois últimos marcadores tratam do funcionamento efetivo do próprio habilitador, e estes indicadores podem ser chamadas de 'indicadores de andamento'.

Para cada habilitador há uma seção separada, que começa com um gráfico semelhante à **figura 27**, mas que inclui diversos elementos do habilitador em questão, indicados em vermelho e em **negrito**.

A seguir, cada um dos quatro componentes é discutido em mais detalhes, abordando componentes específicos e sua relação com os demais habilitadores.

Diversos exemplos também foram incluídos para ilustrar o significado e uso dos habilitadores.

O objetivo desta seção é fornecer mais informações sobre o modelo do COBIT 5 e como o conceito de habilitador pode ser aplicado para implementar e melhorar a governança e gestão de TI da organização.

Habilitador do COBIT 5: Princípios, Políticas e Modelos

Princípios e políticas se referem aos mecanismos de comunicação implementados para transmitir a orientação e as instruções da administração e do órgão de governança. As especificidades do habilitador princípios, políticas e modelos são comparadas com a descrição do habilitador genérico apresentada na **figura 28**.

O modelo do habilitador de princípios, políticas e modelos evidencia:

- **Partes interessadas** – As partes interessadas dos princípios e políticas podem ser internas e externas à organização. Elas incluem o conselho de administração e a diretoria executiva, diretores de conformidade, gerentes de risco, auditores internos e externos, prestadores de serviços, clientes e agências reguladoras. As partes interessadas são de dois tipos: algumas definem e estabelecem políticas, outras devem se alinhar às políticas e cumpri-las.
- **Metas e indicadores** - Princípios, políticas e modelos são instrumentos para transmitir as regras da organização, em apoio aos objetivos de governança e valores da organização, conforme definidos pelo conselho de administração e pela diretoria executiva. Os princípios devem ser:
  - Limitados em número
  - Apresentados em linguagem simples, expressando com o máximo de clareza os valores fundamentais da organização

Políticas fornecem orientação mais detalhada sobre como colocar os princípios em prática e influenciam como a tomada de decisão se alinha aos princípios. Boas políticas são:

- Efetivas - Atingem o objetivo estabelecido.
- Eficientes - Garantem que os princípios sejam implementados da maneira mais eficiente.
- Não intrusivas - Parecem lógicas para aqueles que devem cumpri-las, ou seja, não criam resistência desnecessária.

Políticas de acesso - Há um mecanismo em vigor que proporciona fácil acesso às políticas para todas as partes interessadas? Em outras palavras, as partes interessadas sabem onde encontrar tais políticas?

Figura - 28: Habilitador do COBIT 5: Princípios, Políticas e Modelos

Dimensão do Habilitador

Partes Interessadas
- Partes Interessadas Internas
- Partes Interessadas Externas

Objetivos
- Qualidade Intrínseca
- Qualidade Contextual (relevância, eficácia)
- Assessibilidade e Segurança

Ciclo de Vida
- Planejar
- Projetar
- Desenvolver / Adquirir / Criar / Implementar
- Usar/Operar
- Avaliar / Monitorar
- Atualizar / Descartar

Boas Práticas
- Práticas: Estrutura de Controle, Princípios, Estrutura da política, Escopo e Validade
- Produtos do trabalho (Entradas/Saídas): Declarações das Políticas

Controle do Desempenho do Habilitador

As necessidades das partes interessadas foram atendidas?
As metas do habilitador foram atingidas?
O Ciclo de Vida é Gerenciado?
Boas Práticas Foram Aplicadas?

Indicadores para Atingimento das Metas (Indicadores de Resultado)
Indicadores para Aplicação das Práticas (Indicadores de Desempenho ou Execução)

Modelos de governança e gestão devem fornecer à administração estrutura, orientação, ferramentas, etc., que permitam a governança e gestão adequadas de TI da organização. Os modelos devem ser:

- Abrangentes, cobrindo todas as áreas necessárias
- Abertas e flexíveis, permitindo a adaptação à situação específica da organização
- Atuais, ou seja, refletindo a atual orientação da organização e os atuais objetivos da governança
- Disponíveis e acessíveis a todas as partes interessadas

- **Ciclo de vida** — As políticas têm um ciclo de vida que deve apoiar o atingimento das metas definidas. Os modelos são importantes porque fornecem uma base para definir uma orientação consistente. Por exemplo, um modelo de políticas fornece a base para que um conjunto de políticas consistente possa ser criado e mantido além de oferecer um ponto fácil de navegação dentro e entre cada política.
  Dependendo do ambiente externo em que a organização opera, poderá haver distintos graus de requisitos regulatórios para um controle interno forte e, consequentemente, um modelo de políticas. Um ponto importante a ser observado na consideração dos modelos e políticas é a atualização das políticas — se e quando as políticas são revisadas e atualizadas há fortes mecanismos adotados para garantir que as pessoas estejam cientes de tais atualizações, de que a versão mais nova é facilmente aceita (ver o ponto anterior) e de que as informações obsoletas foram devidamente arquivadas ou descartadas?
- Boas práticas:

- Boas práticas exigem que as políticas façam parte de um modelo geral de governança e gestão, fornecendo um modelo (hierárquico) em que todas as políticas devam caber e fazer claramente a conexão com os princípios subjacentes.
- Como parte do modelo de políticas, os seguintes itens devem ser descritos:
  - Escopo e validade
  - As consequências de não cumprir as políticas
  - Os meios para tratar das exceções
  - A forma com que o cumprimento da política será verificado e medido
- Modelos de governança e gestão de aceitação geral podem fornecer valiosa orientação sobre as afirmações que serão incluídas nas políticas.
- As políticas devem ser alinhadas ao apetite a riscos da organização. As políticas são um componente essencial de um sistema corporativo de controle interno, cujo propósito é administrar e conter o risco. Como parte das atividades de governança de riscos, o apetite da organização a risco é definido, e esse apetite ao risco deve ser refletido nas políticas. Uma organização avessa ao risco tem políticas mais restritas do que uma organização com forte inclinação ao risco.
- As políticas devem ser revalidadas e/ou atualizadas em intervalos regulares.

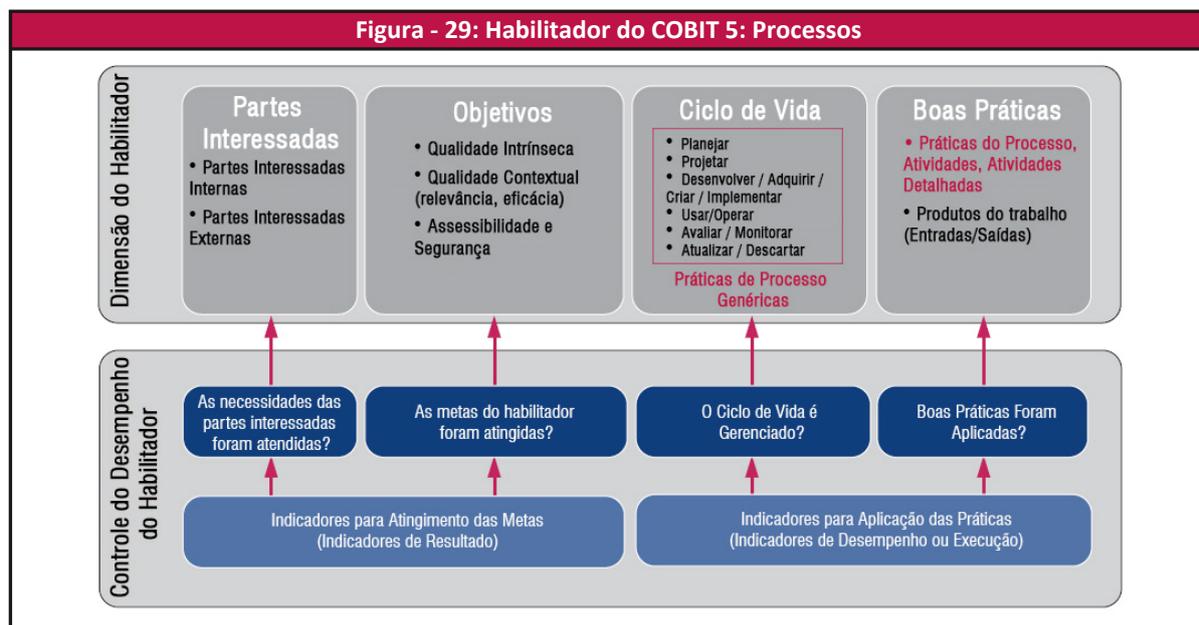
- **Relações com outros habilitadores** — As interações com outros habilitadores incluem:
  - Princípios, políticas e modelos que refletem os valores culturais e éticos da organização, e devem estimular o comportamento desejado; consequentemente, há uma forte ligação desse habilitador com a cultura, a ética e o comportamento.
  - Práticas e atividades dos processos que são o veículo mais importante para a execução das políticas.
  - Estruturas organizacionais que podem definir e implementar as políticas dentro da sua própria abrangência de controle e as suas atividades também são definidas pelas políticas.
  - Políticas que também podem ser informações e, dessa forma, todas as boas práticas que se aplicam às informações também se aplicam às políticas.

EXEMPLO 9 – MÍDIA SOCIAL
Uma organização está considerando como lidar com o rápido aumento da mídia social e a pressão de sua equipe para ter pleno acesso a ela. Até agora, a organização foi conservadora ou restritiva na concessão de acesso a este tipo de serviço, especialmente por motivos de segurança.
Há pressão de todos os lados para rever a posição da organização em relação à média social. Membros da equipe querem níveis de acesso semelhantes aos que têm em suas casas, e a organização em si também deseja usar e explorar os benefícios da mídia social para fins de marketing e sensibilização pública.
A decisão é tomada para definir uma política sobre o uso da mídia social nas redes e sistemas das organizações, inclusive nos laptops fornecidos pela organização aos seus funcionários. A nova política se adapta ao modelo de política existente sob a categoria de “políticas de uso aceitável” e são mais flexíveis do que as políticas anteriores. Como consequência, uma comunicação é desenvolvida para explicar os motivos para essa nova política. Paralelamente, também há um impacto sobre alguns dos demais habilitadores:
Membros da equipe devem aprender como lidar com a nova mídia para evitar situações embaraçosas para a organização. Eles devem aprender o comportamento adequado em consonância com a nova orientação que a organização está tomando e desenvolver as habilidades adequadas.
Diversos processos em relação à segurança devem ser alterados. O acesso é liberado para estas mídias, então as configurações de segurança têm de ser alteradas e possivelmente algumas medidas de compensação deverão ser definidas

Obs.: O COBIT 5 é um exemplo de modelo conforme descrito neste habilitador.

Habilitador do COBIT 5: Processos

As especificidades do habilitador processos são comparadas com a descrição do habilitador genérico e apresentadas na figura 29.

Figura - 29: Habilitador do COBIT 5: Processos

Um processo é definido como **"um conjunto de práticas influenciadas pelas políticas e procedimentos da** organização **que recebe entradas de diversas fontes (inclusive outros processos), que manipula as entradas e produz resultados (por exemplo: produtos, serviços)"**.

A Estrutura do habilitador Processo destaca:

- **Partes interessadas** — Processos têm partes interessadas internas e externas, com seus próprios papéis; as partes interessadas e seus níveis de responsabilidade são documentados nas Tabelas RACI. Partes interessadas externas incluem clientes, parceiros comerciais, acionistas e reguladores. Partes interessadas internas incluem o conselho de administração, as gerências, funcionários e voluntários.
- **Metas** — As metas do processo são definidas como "uma declaração que descreve o resultado esperado de um processo. Um resultado pode ser um artefato, uma mudança significativa de um estado ou uma melhoria significativa na capacidade de outros processos". Elas fazem parte da cascata de objetivos, ou seja, as metas do processo apoiam os objetivos de TI, que por sua vez apoiam os objetivos corporativos.

  As metas do processo podem ser categorizadas como:
  - **Metas intrínsecas** — O processo tem qualidade intrínseca? Ele é exato e está em consonância com as boas práticas? Ele cumpre as normas internas e externas?
  - **Metas contextuais** — O processo foi personalizado e adaptado à situação específica da organização? O processo é significativo, compreensível e fácil de ser aplicado?
  - **Metas de acessibilidade e segurança** — O processo mantém a confidencialidade, quando necessário, é conhecido e está acessível para quem precisa deles?

  Em cada nível da cascata de objetivos, e consequentemente também para os processos, indicadores são definidos para aferir em que medida os objetivos são atingidos. Indicadores podem ser definidos como "uma entidade quantificável que permite medir a consecução da meta de um processo. Os indicadores devem ser SMART (*Specific*, *Measurable*, *Actionable, Relevant and Timely*) — específicos, mensuráveis, acionáveis, pertinentes e tempestivos".

  Para administrar o habilitador de forma eficaz e eficiente, os indicadores devem ser definidos para medir em qual medida os resultados esperados foram atingidos. Além disso, um segundo aspecto do controle de desempenho do habilitador descreve em qual medida as boas práticas foram aplicadas. Aqui também, indicadores associados podem ser definidos para auxiliar no controle do habilitador.
- **Ciclo de vida** — Cada processo tem um ciclo de vida. Ele é definido, criado, operado, monitorado, e ajustado/atualizado ou encerrado. Práticas de processos genéricas tais como as definidas no modelo de avaliação de processos do COBIT com base na ISO/IEC 15504 podem auxiliar na definição, execução, monitoramento e otimização dos processos.
- **Boas práticas** — COBIT 5: Habilitador Processos contém um modelo de referência de processo, que descreve as boas práticas internas do processo com níveis de detalhamento cada vez maiores: Práticas, atividades e atividades detalhadas:[14]

  Práticas:

[14] Somente práticas e atividades são desenvolvidas de acordo com o projeto atual. Os níveis mais detalhados estão sujeitos a desenvolvimento(s) adicional (ais), por exemplo, os diversos guias profissionais podem fornecer orientação mais detalhada para suas áreas. Além disso, orientação adicional pode ser obtida através dos padrões e modelos relacionados, conforme indicado nas descrições detalhadas do processo.

- Para cada processo do COBIT 5, as práticas de governança/gestão fornecem um conjunto completo de requisitos em alto nível para uma governança e gestão de TI da organização prática e eficaz. Elas são:
  - Declarações de ações para realização de benefícios e otimização do nível de risco e o do uso dos recursos
  - Alinhadas aos padrões e boas práticas pertinentes geralmente aceitos
  - Genéricas e, portanto, devem ser adaptadas para cada organização
  - Fazem a cobertura dos atores de TI e de negócios do processo (de ponta a ponta)
- O órgão de governança da organização e a administração devem fazer escolhas relacionadas a estas práticas de governança e gestão:
  - Selecionando as que são aplicáveis e decidindo quais serão implementadas
  - Adicionando e/ou adaptando as práticas conforme necessário
  - Definindo e adicionando práticas não relacionadas à TI para integração aos processos de negócios
  - Escolhendo como implementá-las (frequência, amplitude, automação, etc.)
  - Aceitando o risco de não implementar aquelas que possam ser aplicáveis

Atividades — No COBIT, são principais ações tomadas na operação do processo

- São definidas como "orientação para alcançar as práticas de gestão para obter sucesso na governança e gestão de TI da organização". As atividades do COBIT 5 disponibilizam informações sobre como, por que e o que implementar em cada prática de governança e gestão para melhorar o desempenho da TI e/ou abordar o risco da solução de TI e da prestação de serviço. Este material é útil para:
  - A administração, os prestadores de serviços, os usuários finais e os profissionais de TI que precisam planejar, desenvolver, executar ou monitorar a TI da organização
  - Profissionais de garantia que possam ser questionados sobre suas opiniões em relação às implementações atuais ou propostas ou às melhorias necessárias
- Um conjunto completo de atividades genéricas e específicas que fornecem uma abordagem que inclui todas as etapas necessárias e suficientes para alcançar a principal prática de governança (GP – *Governance Practice*) / prática de gestão (MP – *Management Practice*). Elas fornecem orientação em alto nível, a um nível abaixo do GP/MP para avaliar o desempenho efetivo e considerar potenciais melhorias. As atividades:
  - Descrevem um conjunto de etapas de implementação orientadas às ações necessárias e suficientes para atingir um GP/MP
  - Consideram as entradas e saídas do processo
  - Tem como base os padrões e boas práticas geralmente aceitos
  - Apoiam o estabelecimento de papéis e responsabilidades bem definidos
  - Não são prescritivas e devem ser adaptadas e desenvolvidas em procedimentos específicos adequados à organização

Atividades detalhadas — As atividades podem não ter um nível suficiente de detalhamento para a implementação e uma orientação adicional talvez tenha de ser:

- Obtida a partir de padrões e boas práticas pertinentes específicos tais como ITIL, ISO/IEC série 27000 e PRINCE2
- Desenvolvida como atividades específicas ou mais bem detalhadas como desenvolvimentos adicionais na família de produtos do próprio COBIT 5

Entradas e saídas — As entradas e saídas do COBIT 5 são os produtos do trabalho/artefatos do processo considerados necessários para apoiar a operação do processo. Elas possibilitam decisões importantes, fornecem um registro e uma prova de auditoria das atividades do processo e permitem o acompanhamento em caso de incidente. Elas são definidas em um importante nível da prática de governança/gestão, podem incluir alguns produtos do trabalho usados somente dentro do processo e frequentemente são entradas essenciais para outros processos.[15]

Boas práticas externas podem existir em qualquer forma ou nível de detalhamento e a maioria se refere a outros padrões e modelos. Os usuários podem consultar essas boas práticas externas em todas as ocasiões, visto que o COBIT está alinhado com estes padrões, quando pertinente, e as informações de mapeamento serão disponibilizadas oportunamente.

Controle de Desempenho do Habilitador

Organizações esperam resultados positivos da aplicação e uso dos habilitadores. Para controlar o desempenho dos habilitadores, as perguntas abaixo terão de ser monitoradas e posteriormente respondidas — com base em indicadores — periodicamente:

- As necessidades das partes interessadas foram consideradas?
- As metas do habilitador foram atingidas?
- O ciclo de vida do habilitador é controlado?
- Boas práticas foram aplicadas?

No caso do habilitador Processos, os primeiros dois marcadores tratam do resultado efetivo do processo. Os indicadores usados para mensurar em qual medida as metas foram atingidas podem ser chamados de "indicadores de resultado". No COBIT 5: Habilitador Processo diversos indicadores são definidos para cada meta do processo.

Os dois últimos marcadores tratam do funcionamento real do próprio habilitador e os indicadores para essa finalidade podem ser chamadas de "indicadores de progresso".

[15] As entradas e saídas que ilustram o COBIT 5 não serão consideradas uma lista completa porque fluxos de informações adicionais podem ser definidos, dependendo do ambiente e da estrutura do processo de uma organização específica.

Nível de capacidade do processo — O COBIT 5 possui um esquema de avaliação da capacidade dede processos com base no ISO/IEC 15504. Isto é discutido no capítulo 8 do COBIT 5 e mais orientações estão disponíveis em publicações do ISACA COBIT 5 separadas.

Em suma, o nível de capacidade do processo mede a consecução das metas e a aplicação das boas práticas.

Relações com outros habilitadores — As interações entre os processos e as demais categorias de habilitadores existem através das seguintes relações:

- Processos necessitam de informações (como um dos tipos de entrada) e podem produzir informações (como um produto do trabalho).
- Processos necessitam de estruturas organizacionais e papéis para funcionar, conforme demonstrado nas tabelas RACI. Por exemplo, comitê diretivo de TI, comitê de risco da organização, conselho de administração, auditoria, diretor de TITI, diretor executivo.
- Processos produzem, e também requerem, capacidades de serviço (infraestrutura, aplicativos, etc.)
- Processos podem e irão depender de outros processos.
- Processos produzem ou necessitam de políticas e procedimentos para garantir a consistência da implementação e execução.
- Aspectos culturais e comportamentais determinam a qualidade da execução dos processos.

Exemplo de Habilitador Processo na Prática

O exemplo 10 ilustra o habilitador processo, suas interconexões e as dimensões habilitador. Este exemplo se baseia no exemplo 7 mencionado anteriormente neste documento.

Modelo de Referência de Processo do COBIT 5

PROCESSOS DE GOVERNANÇA E GESTÃO

Um dos princípios que norteiam o COBIT 5 é a distinção feita entre governança e gestão. Em consonância com este princípio, seria esperado que todas as organizações implementassem diversos processos de governança e diversos processos de gestão que forneceriam a governança e gestão de TI geral da organização.

Ao considerar os processos de governança e gestão no contexto da organização, a diferença entre os tipos de processos reside nos seus objetivos:

- Processos de governança — Os processos de governança tratam dos objetivos de governança das partes interessadas, para a criação de valor, e otimização dos riscos e dos recursos — e incluem práticas e atividades voltadas à avaliação das opções estratégicas, fornecendo orientação para a TI e monitorando o resultado (EDM - *Evaluate, Direct, and Monitor* - Avaliar, Dirigir e Monitorar, - em consonância com os conceitos do padrão ISO/IEC 38500).
- Processos de gestão — Em consonância com as definições de gestão, práticas e atividades dos processos de gestão cobrem as áreas de responsabilidade de PBRM (*Plan, Build, Run, and Monitor*) de TI da organização e devem fornecer cobertura de TI de ponta a ponta.

EXEMPLO 10 — INTERCONEXÕES DO HABILITADOR DE PROCESSO
Uma organização nomeou 'gerentes de processo' de TI encarregados de definir e operar processos de TI eficientes e eficazes no contexto da boa governança e gestão de TI da organização. Primeiramente, os gerentes de processo se concentrarão no habilitador de processo, considerando as dimensões do habilitador: **Partes interessadas**: Partes interessadas do processo incluem todos os atores do processo, ou seja, todas as partes responsáveis, consultadas ou informadas (RACI) sobre, ou durante, as atividades do processo. Para tanto, a tabela RACI descrita no COBIT 5: *Enabling Processes* poderá ser utilizada. **Metas**: Cada processo deve definir metas adequadas com indicadores correspondentes. Por exemplo, para o processo APO08 Gerenciar Relacionamentos (in COBIT 5: *Enabling Processes*) pode-se encontrar um conjunto de metas e indicadores de processo tais como: – Meta: Estratégias de negócio, planos e requerimentos são bem documentados, entendidos e aprovados. • Indicador: Percentual de programas alinhados com os requisitos/prioridades de negócios da organização. – Meta: Existência de bons relacionamentos entre a organização e o departamento de TI. • Indicador: Classificações de usuário e pesquisas de satisfação do pessoal de TI. **Ciclo de Vida:** Cada processo tem um ciclo de vida, ou seja, ele deve ser criado, executado, monitorado e ajustado conforme necessário. Eventualmente, o processo deixa de existir. Neste caso, os gerentes de processo terão de conceber e definir o processo em primeiro lugar. Eles podem usar vários elementos do COBIT 5: *Enabling Processes* para conceber os processos, ou seja, definir responsabilidades e desmembrar o processo em práticas e atividades, bem como definir os produtos do trabalho do processo (entradas e saídas). Em um segundo momento, o processo deverá ser criado de forma mais sólida e eficiente e para isso os gerentes de processo podem elevar o nível de capacidade do processo. O Modelo de Capacidade de Processo do COBIT 5 inspirado no ISO/IEC 15504 e os atributos de capacidade do processo podem ser usados para essa finalidade, tais como: -- A capacidade de processo nível 2 exige a consecução de dois atributos: Controle de Desempenho e Gestão do Produto do Trabalho. O primeiro atributo exige diversas atividades relacionadas com a fase de planejamento: • Definição das metas de desempenho do processo. • Planejamento do desempenho do processo. • Definição das responsabilidades pela execução do processo. • Identificação dos recursos. • Etc. O mesmo nível de capacidade prescreve diversas atividades para a fase de "monitoramento" do ciclo de vida do processo tais como: • Monitoramento do desempenho do processo. • Ajuste do desempenho do processo para atender ao planejamento. • Etc. – A mesma abordagem pode ser utilizada para obter orientação para as diferentes fases do ciclo de vida a partir de diferentes atributos de capacidade de desempenho em níveis mais altos da capacidade do processo. **Boa prática:** O COBIT 5 descreve de forma bastante detalhada as boas práticas de processos no COBIT 5: *Enabling Processes*, conforme mencionado no item anterior. Inspiração e exemplos de processos podem ser encontrados ali, cobrindo todo o espectro de atividades necessárias para a boa governança e gestão de TI da organização. Além de orientação sobre o habilitador processo, os gerentes de processo podem decidir observar diversos outros habilitadores tais como: As tabelas RACI, que descrevem os papéis e responsabilidades. Outros habilitadores permitem aprofundar-se nesta dimensão, tais como: - No habilitador habilidades e competências, as habilidades e competências necessárias em cada papel podem ser definidas e metas apropriadas (por exemplo: níveis de habilidade técnica e comportamental) e seus respectivos indicadores podem ser definidas. - A tabela RACI também contém diversas estruturas organizacionais. Essas estruturas podem ser mais bem elaboradas no habilitador de estruturas organizacionais, onde uma descrição mais detalhada da estrutura pode ser encontrada, resultados esperados e seus respectivos indicadores podem ser definidos (por exemplo: decisões) e boas práticas podem ser definidas (por exemplo: abrangência do controle, princípios operacionais da estrutura, nível de autoridade). Princípios e políticas formalizarão os processos e prescreverão porque o processo existe, a quem se aplica e como o processo deverá ser usado. Esta é a área de enfoque do habilitador políticas e princípios.

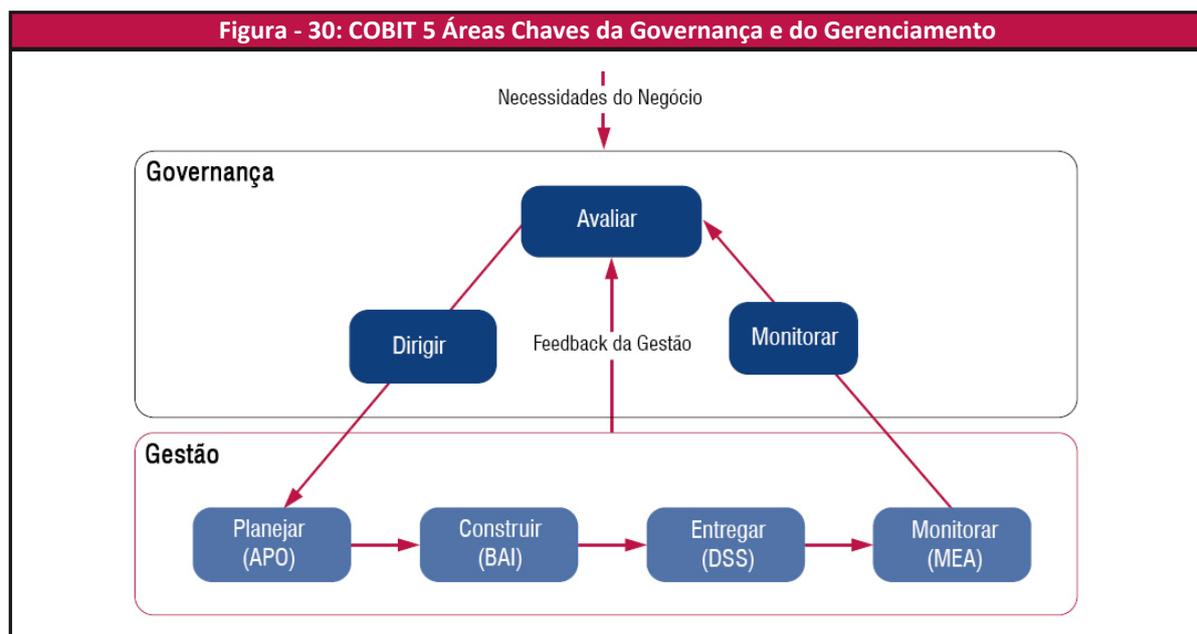
Embora o resultado dos tipos de processos seja diferente e destinado a um público diverso, internamente, no contexto do processo em si, todos os processos requerem atividades de "planejamento", "construção, desenvolvimento ou implementação", "entrega" e "monitoramento" das atividades do processo.

Modelo de Referência de Processo do COBIT 5

O COBIT 5 não é prescritivo, mas no texto acima fica claro que ele defende que as organizações implementem processos de governança e gestão de tal forma que as principais áreas sejam cobertas, conforme demonstrado na figura 30.

Na teoria, uma organização pode organizar seus processos conforme julgar adequado, contanto que todos os objetivos de governança e gestão necessários sejam cobertos. Organizações de menor porte podem ter menos processos; organizações de maior porte e mais complexas poderão ter muitos processos, todos para cobrir os mesmos objetivos.

Figura - 30: COBIT 5 Áreas Chaves da Governança e do Gerenciamento

Necessidades do Negócio
Governança
Avaliar
Dirigir
Feedback da Gestão
Monitorar
Gestão
Planejar (APO)
Construir (BAI)
Entregar (DSS)
Monitorar (MEA)

Não obstante o texto anterior, o COBIT 5 inclui um modelo de referência de processo, que define e descreve em detalhes diversos processos de governança e gestão. Isso fornece um modelo de referência de processo que representa todos os processos normalmente encontrados nas atividades de TI de uma organização, oferecendo um modelo de referência comum compreensível aos administradores operacionais de TI e administradores de negócios. O modelo de processo proposto é um modelo completo e abrangente, mas não é o único modelo de processo possível. Cada organização deve definir seu próprio conjunto de processos, considerando sua situação específica.

Incorporar um modelo operacional e uma linguagem comum para todas as partes da organização envolvidas nas atividades de TI é uma das etapas mais importantes e críticas da boa governança. Isso também fornece uma estrutura para medição e monitoramento do desempenho de TI, comunicação com os prestadores de serviços e integração das melhores práticas de gestão.

O modelo de referência de processo do COBIT 5 subdivide os processos de governança e gestão de TI da organização em duas áreas de atividades principais — governança e gestão — divididas em dois domínios de processos:

- **Governança** — Este domínio contém cinco processos de governança e práticas de EDM são definidas dentro de cada processo.
- **Gestão** — Estes quatro domínios estão em consonância com as áreas de responsabilidade de PBRM (uma evolução dos domínios do COBIT 4.1) e proporcionam uma cobertura de TI de ponta a ponta. Cada domínio contém diversos processos, como no COBIT 4.1 e versões anteriores. Embora, conforme já mencionado, a maioria dos processos requeira atividades para "planejar", "construir", "entregar" e "monitorar" o processo ou o problema específico a ser abordado (por exemplo, qualidade e segurança), eles são alocados em domínios de acordo com a área de atividade mais relevante em relação a TI da organização.

No COBIT 5 os processos também cobrem o escopo completo dos negócios e atividades de governança e gestão de TI da organização, levando o modelo do processo efetivamente para toda a organização.

O modelo de referência de processo do COBIT 5 é o sucessor do modelo de processo do COBIT 4.1, e conta ainda com a integração dos modelos de processo do Risk IT e do Val IT. A figura 31 mostra o conjunto completo de 37 processos de governança e de gestão do COBIT 5. Os detalhes de todos os processos, de acordo com o modelo de processo descrito previamente, foram incluídos no COBIT 5*:* Habilitador Processo.

Figura - 31: COBIT 5 Modelo de Referência de Processos

Processos de Governança Corporativa de TI

Avaliar, Dirigir e Monitorar

EDM01 Garantir a Definição e Manutenção do Modelo de Governança
EDM02 Garantir a Realizacao de Beneficios
EDM03 Garantir a Otimização do Risco
EDM04 Garantir a Otimização dos Recursos
EDM 05 Garantir Transparência para as Partes Interessadas

Alinhar, Planejar e Organizar

APO01 Gerenciar a Estrutura de Gestao de TI
APO02 Gerenciar a Estrategia
APO03 Gerenciar Arquitetura da Organizacao
APO04 Gerenciar Inovação
APO05 Gerenciar Portfolio
APO06 Gerenciar Orcamento e Custos
APO07 Gerenciar Recursos Humanos
APO08 Gerenciar Relacionamentos
APO09 Gerenciar Contratos de Prestação de Serviços
APO10 Gerenciar Fornecedores
APO11 Gerenciar Qualidade
APO12 Gerenciar Riscos
APO13 Gerenciar Segurança

Construir, Adquirir e Implementar

BAI01 Gerenciar Programas e Projetos
BAI02 Gerenciar Definição de Requisitos
BAI03 Gerenciar Identificacao e Desenvolvimento de Solucoes
BAI04 Gerenciar Disponibilidade e Capacidade
BAI05 Gerenciar Capacidade de Mudanca Organizacional
BAI06 Gerenciar Mudancas
BAI07 Gerenciar Aceitacao e Transicao da Mudanca
BAI08 Gerenciar Conhecimento
BAI09 Gerenciar Ativos
BAI10 Gerenciar Configuracao

Entregar, Serviço e Suporte

DSS01 Gerenciar Operações
DSS02 Gerenciar Solicitações e Incidentes de Serviços
DSS03 Gerenciar Problemas
DSS04 Gerenciar Continuidade
DSS05 Gerenciar Serviços de Segurança
DSS06 Gerenciar Controles do Processo de Negócio

Monitorar, Avaliar e Analisar

MEA01 Monitorar, Avaliar e Analisar Desempenho e Conformidade
MEA02 Monitorar, Avaliar e Analisar o Sistema de Controle Interno
MEA03 Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos

Processos para Gestão Corporativa de TI

Habilitador do COBIT 5: Estruturas Organizacionais

As especificidades do habilitador estruturas organizacionais são comparadas com a descrição do habilitador genérico e apresentadas na figura 32.

O modelo do habilitador estruturas organizacionais evidencia:

- **Partes interessadas** — No caso de estruturas organizacionais as partes Interessadas podem ser internas e externas à organização e incluem cada membro da estrutura, outras estruturas, entidades organizacionais, clientes, fornecedores e reguladores. Seus papéis variam e incluem tomadas de decisão, influência e assessoramento. Os interesses de cada uma das partes Interessadas também podem variar, ou seja, quais interesses elas têm nas decisões tomadas pela estrutura?
- **Metas** — As metas do próprio habilitador estruturas organizacionais também teriam sua própria ordem, princípios operacionais bem definidos e aplicação de outras boas práticas. O resultado do habilitador de estruturas organizacionais deveria incluir diversas atividades e decisões.
- **Ciclo de vida** — Cada estrutura organizacional tem um ciclo de vida. Ela é criada, colocada em operação, ajustada e, por fim, pode ser descartada. Durante sua criação, uma ordem — um motivo e objetivo para sua existência — deve ser definida.
- **Boas práticas** — Diversas boas práticas para estruturas organizacionais podem ser destacadas, tais como:
  - Princípios operacionais — As disposições práticas sobre como a estrutura operará, a frequência de reuniões, normas de documentação e organização.
  - Composição — As estruturas são formadas por membros, que podem partes interessadas internas ou externas.
  - Abrangência de controle — Os limites dos direitos de decisão da estrutura organizacional
  - Nível de autoridade/direitos de decisão — As decisões que a estrutura está autorizada a tomar
  - Delegação de autoridade — A estrutura pode delegar (um subconjunto de) seus direitos de decisão a outras estruturas que se reportem a ela.
  - Procedimentos de escalação — O caminho da escalação de uma estrutura descreve as ações necessárias no caso de problemas com a tomada de decisão.

Figura - 32: Habilitador do COBIT 5: Estrutura Organizacional

Dimensão do Habilitador
Partes Interessadas
• Partes Interessadas Internas
• Partes Interessadas Externas
Objetivos
• Qualidade Intrínseca
• Qualidade Contextual (relevância, eficácia)
• Assessibilidade e Segurança
Ciclo de Vida
• Planejar
• Projetar
• Desenvolver / Adquirir / Criar / Implementar
• Usar/Operar
• Avaliar / Monitorar
• Atualizar / Descartar
Boas Práticas
• Práticas: Princípios Operacionais, Amplitude de Controle (Escopo), Nível de Autoridade, Delegação de Autoridade Processos de Escalação
• Produtos do trabalho (Entradas/Saídas): Decisões
Controle do Desempenho do Habilitador
As necessidades das partes interessadas foram atendidas?
As metas do habilitador foram atingidas?
O Ciclo de Vida é Gerenciado?
Boas Práticas Foram Aplicadas?
Indicadores para Atingimento das Metas (Indicadores de Resultado)
Indicadores para Aplicação das Práticas (Indicadores de Desempenho ou Execução)

Relações com outros habilitadores — As interações com outros habilitadores incluem:

Tabelas RACI associam as atividades do processo às estruturas organizacionais e/ou papéis individuais na organização. Elas descrevem o nível de envolvimento de cada papel em cada prática de processo: Responsável, Aprovador, Consultado ou Informado.

- Cultura, ética e comportamento determinam a eficiência e eficácia das estruturas organizacionais e de suas decisões.
- A composição das estruturas organizacionais deverá ser levada em consideração e isso exige um conjunto de habilidades adequadas de seus membros.
- Os princípios de ordem e operação das estruturas organizacionais são orientados pelos modelos de políticas adotado.
- Entradas e saídas — Uma estrutura requer entradas (geralmente informações) antes que ela possa tomar decisões com base em informações e isso produz saídas, por exemplo, decisões, outras informações ou solicitações de entradas adicionais.

Ilustração das Estruturas Organizacionais do COBIT 5

Conforme mencionado na discussão sobre o modelo de processo do COBIT 5, um modelo de referência de processo do COBIT 5 foi criado e é descrito em detalhes no COBIT 5*:* Habilitador Processo. O modelo inclui Tabelas RACI, que utilizam diversos papéis e estruturas. A figura 33 descreve estes papéis e estruturas predefinidos.

Observações:

- Elas não devem necessariamente corresponder aos papéis reais que as organizações implementaram, mas, não obstante, agregam valor no sentido de que o objetivo descrito da estrutura ou papel continue válido para a maioria das organizações.
- A finalidade desta tabela não é prescrever uma tabela organizacional universal para cada organização. Em vez disso, ela deve ser vista como uma ilustração.

Figura - 33: Papéis e Estruturas Organizacionais

Papel/Estrutura	Definição/Descrição
Conselho de Administração	O grupo de executivos mais antigos e/ou conselheiros não executivos da organização responsáveis pela governança da organização e controle geral dos seus recursos
Diretor Executivo (Presidente)	Diretor com o maior nível de autoridade, responsável pela administração da organização como um todo
Diretor Financeiro	O diretor mais graduado da organização na área, responsável por todos os aspectos da administração financeira, inclusive riscos e controles financeiros bem como pela confiabilidade e exatidão das contas
Diretor de Operações	O diretor mais graduado da organização na área, responsável pela operação da organização
Diretor de Riscos	O diretor mais graduado da organização na área, responsável por todos os aspectos da gestão de risco da organização. A função do diretor de risco de TI pode ser criada para supervisionar os riscos de TI
Diretor de TI	O diretor mais graduado da organização na área, responsável pelo alinhamento de TI com as estratégias de negócios e responsável pelo planejamento, mobilização de recursos e administração da prestação de serviços e soluções de TI em apoio aos objetivos corporativos
Diretor de Segurança da Informação	O diretor mais graduado da organização na área, responsável pela segurança das informações da organização em todas as suas formas
Executivo de Negócios	O administrador sênior responsável pela operação de uma unidade de negócios ou subsidiária específica
Responsável pelo Processo de Negócios	Pessoa responsável pela execução de um processo e consecução de seus objetivos, orientação de melhorias no processo e aprovação de mudanças no processo
Comitê Estratégico (Executivo Estratégico de TI)	Grupo de executivos seniores nomeados pelo conselho de administração para garantir que o conselho participe e seja informado sobre as principais questões e decisões de TI. O comitê é responsável pela administração dos portfólios de investimentos habilitados pela TI, serviços de TI e ativos de TI, garantindo a criação de valor e a gestão de riscos. O comitê é geralmente presidido por um membro do conselho e não pelo Diretor de TI.
Comitês Diretivos (Projeto e Programa)	Grupo departes interessadas e especialistas responsáveis pela orientação de programas e projetos, inclusive monitoramento e administração de planos, alocação de recursos, realização de benefícios e criação de valor bem como a gestão do risco do programa e do projeto
Conselho de Arquitetura	Grupo departes interessadas e especialistas responsáveis pela orientação dos assuntos e decisões sobre a arquitetura corporativa da organização e pela definição das políticas e padrões arquitetônicos
Comitê de Riscos da Organização	Grupo de executivos da organização responsáveis pela colaboração em nível organizacional e pelo consenso exigido para apoiar as atividades e decisões da governança de riscos organizacionais (ERM – *Enterprise Risk Management*). Um conselho de risco de TI pode ser criado para considerar os riscos de TI de forma mais detalhada e aconselhar o comitê de riscos da organização
Chefe de RH	O diretor mais graduado de uma organização na área responsável pelo planejamento e pelas políticas de recursos humanos daquela organização
Conformidade	Papel na organização responsável pela orientação sobre a conformidade legal, regulatória e contratual
Auditor	Papel na organização responsável pela realização de auditorias internas
Chefe de Arquitetura	Funcionário mais graduado responsável pelos processos de arquitetura da organização
Chefe de Desenvolvimento	Funcionário mais graduado responsável pelos processos de desenvolvimento de soluções de TI
Chefe de Operações de TI	Funcionário mais graduado responsável pelos ambientes operacionais e pela estrutura de TI

Figura – 33: Papéis e Estruturas Organizacionais (cont)	
Papel/Estrutura	**Definição/Descrição**
Chefe de Administração de TI	Funcionário graduado responsável pelos registros de TI e pelos assuntos administrativos relacionados à TI
Escritório de Programas e Projetos (PMO)	Órgão responsável pelo apoio aos gerentes de programa e de projeto, levantamento, avaliação e relatório das informações sobre a conduta de seus programas e projetos constituintes
Escritório de Gestão do Valor da Organização (VMO)	Órgão que atua na gestão de portfólios de investimentos e serviços, inclusive avaliando e aconselhando sobre oportunidades de investimentos e estudos de caso, recomendando métodos e controles de valores de governança/gestão e informando sobre o progresso na sustentação e criação de valores gerados pelos investimentos e serviços
Gerente de Serviços	Pessoa que gerencia o desenvolvimento, implementação, avaliação e o controle contínuo de produtos e serviços novos e já existentes para um cliente específico (usuário) ou grupo de clientes (usuários)
Gerente de Segurança da Informação	Pessoa que administra, projeta, prevê e/ou avalia a segurança da informação de uma organização
Gerente de Continuidade dos Negócios	Pessoa que administra, projeta, prevê e/ou avalia a capacidade de continuidade dos negócios de uma organização para garantir que as funções críticas daquela empresa continuem a operar após eventos de interrupção
Diretor de Privacidade	Pessoa responsável pelo monitoramento dos riscos e impacto nos negócios de leis de privacidade, e pela orientação e coordenação da implementação de políticas e atividades que garantam que as diretrizes de privacidade serão cumpridas. Também conhecido como diretor de proteção de dados.

Habilitador do COBIT 5: Cultura, Ética e Comportamento

Cultura, ética e comportamento referem-se ao conjunto de comportamentos individuais e coletivos de cada organização.

As especificidades do habilitador cultura, ética e comportamento são comparadas com a descrição do habilitador genérico e apresentadas na figura 34.

Figura - 34: Habilitador do COBIT 5: Cultura, Ética e Comportamento

Dimensão do Habilitador

Partes Interessadas
• Partes Interessadas Internas
• Partes Interessadas Externas

Objetivos
• Qualidade Intrínseca
• Qualidade Contextual (relevância, eficácia)
• Assessibilidade e Segurança

Ciclo de Vida
• Planejar
• Projetar
• Desenvolver / Adquirir / Criar / Implementar
• Usar/Operar
• Avaliar / Monitorar
• Atualizar / Descartar

Boas Práticas
• Práticas: Comunição
Execução
Incentivos e Recompensas
Conscientização
Regras e Normas
Liderança
• Produtos do trabalho (Entradas/Saídas)

Controle do Desempenho do Habilitador

As necessidades das partes interessadas foram atendidas?
As metas do habilitador foram atingidas?
O Ciclo de Vida é Gerenciado?
Boas Práticas Foram Aplicadas?

Indicadores para Atingimento das Metas (Indicadores de Resultado)
Indicadores para Aplicação das Práticas (Indicadores de Desempenho ou Execução)

O modelo do habilitador cultura, ética e comportamento evidencia:

- **Partes interessadas** — As partes interessadas do habilitador cultura, ética e comportamento podem ser internas e externas à organização. Partes interessadas internas incluem toda a organização, partes interessadas externas incluem reguladores, por exemplo, auditores externos ou órgãos de fiscalização. Há dois tipos de interesses: Algumas partes interessadas, por exemplo, representantes legais, gerentes de risco, administradores de RH, conselhos e diretores de remuneração, tratam da definição, implementação e execução dos comportamentos desejados e os demais devem alinhar-se às normas e regulamentos definidos.
- **Metas** — As metas do habilitador cultura, ética e comportamento se referem a:
  - Ética organizacional, determinada pelos valores que nortearão a existência da organização
  - Ética individual, determinada pelos valores pessoais de cada funcionário da organização e dependente, em uma importante medida, de fatores externos como religião, etnia, contexto socioeconômico, geografia e experiências pessoais
  - Comportamentos individuais, que determinam coletivamente a cultura de uma organização. Diversos fatores, tais como os fatores externos mencionados acima, além das relações interpessoais nas organizações, objetivos e ambições pessoais, orientam o comportamento. Alguns tipos de comportamentos que podem ser significativos neste contexto incluem:
  - Comportamento relativo à assunção de riscos — Em que medida a organização sente que pode absorver riscos e quais riscos ela está disposta a assumir?
  - Comportamento relativo à adoção de políticas — Em que medida as pessoas adotarão e/ou cumprirão a política?
  - Comportamento no caso de resultados negativos — Como a organização lida com resultados negativos, ou seja, prejuízos ou até mesmo perda de oportunidades? Ela aprende com essas perdas e tenta melhorar ou a culpa será atribuída sem tratar da causa raiz?
- **Ciclo de vida** —Cultura organizacional, postura ética e comportamento individual, etc., todos possuem seus ciclos de vida. Partindo da cultura existente, uma organização pode identificar as mudanças necessárias e trabalhar em sua implementação. Diversas ferramentas — descritas nas boas práticas — podem ser utilizadas.
- **Boas práticas** —Boas práticas para criação, incentivo e manutenção do comportamento desejado:
  - Comunicação para toda a organização dos comportamentos desejados e valores corporativos subjacentes
  - Conscientização do comportamento desejado, reforçada por um exemplo de comportamento exercido pela alta administração e outras lideranças
  - Incentivos para encorajar e convencer a adotar o comportamento desejado. Há uma conexão clara entre o comportamento individual e o esquema de recompensas de RH adotado pela organização.
  - Regulamentos e normas, que fornecem mais orientação sobre o comportamento organizacional desejado. Isso conecta de forma muita clara os princípios e políticas adotados pela organização.
- **Relações com outros habilitadores** — As interações com outros habilitadores incluem:
  - Processos podem ser concebidos em um nível de perfeição, mas se as partes interessadas do processo não desejarem executar as atividades do processo conforme esperado — por exemplo, se seu comportamento não estiver em conformidade, os resultados do processo não serão alcançados.

- Do mesmo modo, estruturas organizacionais podem ser projetadas e criadas de acordo com o manual, mas se suas decisões não forem implementadas — por motivos de agendas pessoais diferentes, falta de incentivos, etc. — elas não resultarão em uma governança e gestão de TI da organização aceitável.
- Princípios e Políticas são um mecanismo de comunicação muito importante para os valores corporativos e o comportamento desejado.

EXEMPLO 11 — MELHORIA DA QUALIDADE

Uma organização enfrenta repetidamente sérios problemas de qualidade com novos aplicativos. Apesar do fato de uma sólida metodologia de desenvolvimento de projeto de software ter sido adotada, muitas vezes os problemas com o software geram problemas operacionais no cotidiano da organização.

Uma pesquisa mostrou que os membros da equipe de desenvolvimento e a administração são avaliados e recompensados com base na pontualidade da entrega, dentro do orçamento, de seus projetos. Eles não são avaliados por critérios de qualidade ou critérios de benefícios para a organização. Consequentemente, eles se concentram diligentemente no prazo de entrega e na redução de custos durante o desenvolvimento, por exemplo, tempo dos testes. A pesquisa mostrou também que o cumprimento da metodologia e dos procedimentos estabelecidos praticamente não existe, uma vez que ela exigiria um pouco mais de tempo no desenvolvimento do orçamento (a favor da qualidade). Além disso, a estrutura organizacional é de tal forma que o envolvimento da área de desenvolvimento cessa uma vez que o desenvolvimento é transferido para a equipe de operações. A partir daí, o envolvimento com a área de desenvolvimento é somente indireto, por meio dos processos criados para controle de incidentes e controle de problemas.

A lição aprendida é que os melhores incentivos devem ser usados para solucionar a administração do desenvolvimento e incentivar as equipes melhorarem a qualidade do trabalho.

EXEMPLO 12 — RISCO DE TI

Alguns sintomas de uma cultura inadequada ou problemática em relação aos riscos de TI incluem:

Desalinhamento entre a real inclinação ao risco e a sua conversão em políticas. Os reais valores da administração em relação aos riscos podem ser razoavelmente agressivos e de assunção de riscos, ao passo que as políticas criadas refletem uma atitude muito mais conservadora. Por isso, há uma incompatibilidade entre os valores e os meios para se compreender esses valores, levando inevitavelmente ao conflito. Conflitos podem surgir, por exemplo, entre os incentivos definidos para a administração e a execução de políticas desalinhadas.

A existência de uma "cultura de culpa". Este tipo de cultura deve ser evitado de todas as formas; ela é o mais eficaz inibidor de comunicação significativa e eficaz. Em uma cultura de culpa, as unidades de negócios tendem a apontar o dedo para TI quando os projetos não são entregues no prazo ou não atendem às expectativas. Ao fazê-lo, elas não conseguem perceber como o envolvimento das unidades de negócios no início do projeto afeta o sucesso do processo. Em casos extremos, a unidade de negócios pode assumir a culpa por não atender às expectativas que a unidade nunca comunicou claramente. O "jogo de culpa" só prejudica a comunicação eficaz entre as unidades, fazendo aumentar os atrasos. A liderança executiva deve identificar e controlar rapidamente a cultura de culpa se a colaboração for fomentada em toda a organização.

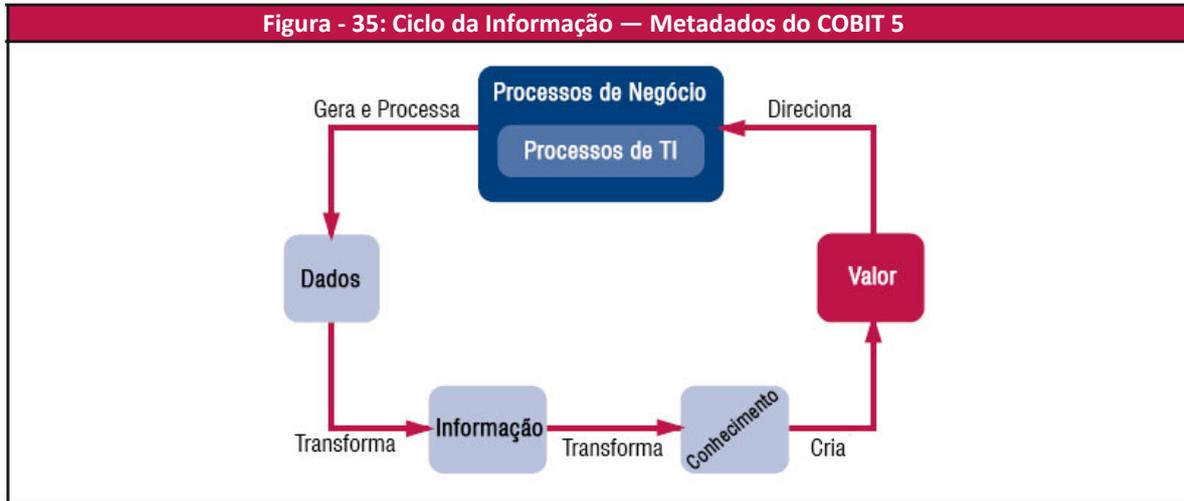
Habilitador do COBIT 5: Informação

Introdução — O Ciclo da Informação

O habilitador informação trata das informações importantes para as organizações e não apenas das informações automatizadas. As informações podem ser estruturadas ou desestruturadas, formalizadas ou não formalizadas.

A informação pode ser considerada uma etapa do "ciclo da informação" de uma organização. No ciclo da informação (figura 35), os processos de negócios geram e processam os dados, transformando-os em informações e conhecimento e, por fim, criam valor para a organização. O escopo do habilitador informação refere-se principalmente à fase de "informação" no ciclo da informação, mas os aspectos dos dados e do conhecimento também são cobertos pelo COBIT 5.

Figura - 35: Ciclo da Informação — Metadados do COBIT 5

Processos de Negócio
Processos de TI
Gera e Processa
Direciona
Dados
Valor
Transforma
Informação
Transforma
Conhecimento
Cria

Habilitador informação do COBIT 5

As especificidades do habilitador informação são comparadas com a descrição do habilitador genérico e apresentadas na figura 36.

Figura - 36: Habilitador do COBIT 5: Informação

Dimensão do Habilitador

Partes Interessadas
- Partes Interessadas Internas
- Partes I nteressadas Externas

Objetivos
- Qualidade Intrínseca
- Qualidade Contextual (relevância, eficácia)
- Assessibilidade e Segurança

Ciclo de Vida
- Planejar
- Projetar
- Desenvolver / Adquirir / Criar / Implementar
- Usar/Operar
- Avaliar / Monitorar
- Atualizar / Descartar

Boas Práticas
- Práticas: Definem os Atributos da informação
- Físicos (Veículo, Mídia)
- Empíricos (Interface do Usuário)
- Sintáticos (Linguagem, Formato)
- Semânticos (Significado), Tipo, Atualização, Nível
- Pragmáticos (Uso), Inclui Retenções, Status, Contingência, Inovação
- Sociais (Contexto)

Controle do Desempenho do Habilitador

As necessidades das partes interessadas foram atendidas?
As metas do habilitador foram atingidas?
O Ciclo de Vida é Gerenciado?
Boas Práticas Foram Aplicadas?
Indicadores para Atingimento das Metas (Indicadores de Resultado)
Indicadores para Aplicação das Práticas (Indicadores de Desempenho ou Execução)

O modelo do habilitador informação (IM) destaca:

- **Partes interessadas** — Podem ser internas ou externas à organização. O modelo genérico também sugere que, além de identificar as partes interessadas, seus interesses devem ser identificados, ou seja, por que eles se preocupam ou estão interessados na informação.

Ao considerar para qual parte interessada a informação será destinada, diferentes categorias de funções de tratamento da informação são possíveis, variando desde as propostas detalhadas — por exemplo, sugerindo dados específicos ou funções que tratam da informação tais como arquiteto, responsável, administrador, fiduciário, fornecedor, beneficiário, modelador, gerente de qualidade, gerente de segurança — para propostas mais gerais — por exemplo, diferenciando entre produtores, custodiantes e clientes da informação:

- Produtor de informação, responsável pela geração da informação
- Custodiante de informação, responsável pela salvaguarda da informação
- Cliente de informação, responsável pelo uso da informação

Estas categorias se referem às atividades específicas relacionadas às fontes de informação. As atividades dependem da fase do ciclo de vida da informação; no entanto, para encontrar uma categoria de papéis que possua um nível adequado de granularidade para o IM, a dimensão do ciclo da informação do IM pode ser utilizada. Isso significa que os papéis das partes interessadas da informação podem ser definidos de acordo com a fase do ciclo da informação, por exemplo, planejadores da informação, receptores da informação e usuários da informação. Paralelamente, isso significa que a dimensão das partes interessadas da informação não é uma dimensão independente; cada fase do ciclo de vida terá partes interessadas diferentes.

Considerando que os papéis significativos dependem da fase do ciclo de vida da informação, as partes interessadas podem ter relação com as metas da informação.

- **Metas** — As metas da informação são divididas em três subdimensões de qualidade:
  - **Qualidade intrínseca** — Em que medida os valores dos dados estão em conformidade com os valores reais e efetivos. Isso inclui:
    - Exatidão — Em que medida a informação é correta e confiável
    - Objetividade — Em que medida a informação é imparcial e sem preconceitos
    - Credibilidade — Em que medida a informação é considerada verdadeira e credível
    - Reputação — Em que medida a informação é altamente considerada em termos de sua fonte ou conteúdo
  - **Qualidade contextual e representacional** — Em que medida a informação é aplicável à tarefa do usuário da informação e é apresentada de forma clara e inteligível, reconhecendo que a qualidade da informação depende do contexto do uso. Isso inclui:
    - Relevância — Em que medida a informação é aplicável e útil à tarefa em questão
    - Completude — Em que medida a informação é completa e abrangente o suficiente para a tarefa em questão
    - Atualização — Em que medida a informação está suficientemente atualizada para a tarefa em questão
  - **Quantidade correta de Informação** — Em que medida o volume de Informação é adequado para a tarefa em questão
    - Representação concisa — Em que medida a informação é representada de forma compacta
    - Representação consistente — Em que medida a informação é apresentada no mesmo formato
    - Interpretabilidade — Em que medida a informação é apresentada em linguagens, símbolos e unidades adequados, com definições claras
    - Compreensibilidade — Em que medida a informação é facilmente compreendida
    - Facilidade de manipulação — Em que medida a informação é facilmente manipulada e aplicada a diferentes tarefas
    - Segurança/qualidade da acessibilidade — Em que medida a informação é disponibilizada e obtida. Isso inclui:
    - Disponibilidade/agilidade — Em que medida a informação é disponibilizada quando necessário, ou fácil e rapidamente recuperável
    - Acesso restrito — Em que medida o acesso à informação é restrito adequadamente às partes autorizadas

  O Apêndice F fornece uma descrição detalhada sobre como os critérios de qualidade de Informação do COBIT 5 são comparados com os critérios de Informação do COBIT 4.1. Por exemplo, a integridade (conforme definição no COBIT 4.1) é coberta pelas metas de completude e exatidão da informação.
- **Ciclo de Vida** — O ciclo de vida completo da informação deve ser considerado e diferentes abordagens podem ser necessárias para a informação nas diferentes fases do ciclo de vida. O habilitador de informação do COBIT 5 destaca as seguintes fases:
  - Planejar — A fase em que a criação e o uso dos recursos da informação são preparados. As atividades desta fase podem se referir à identificação dos objetivos, ao planejamento da arquitetura da informação e à elaboração dos padrões e definições como, por exemplo, definições dos dados e dos procedimentos de coleta de dados.
  - Projetar
  - Desenvolver/adquirir — A fase em que os recursos de informação são adquiridos. As atividades desta fase podem se referir à criação dos registros de dados, compra de dados e carregamento de arquivos externos.
  - Usar/operar, que inclui:
  - Armazenamento — A fase em que a informação é armazenada eletronicamente ou em cópia impressa (ou até mesmo na memória humana). As atividades desta fase podem se referir ao armazenamento da informação em forma eletrônica (por exemplo, em arquivos eletrônicos, bancos de dados, *Data Warehouses*) ou em cópia impressa (por exemplo, documentos em papel).
  - Compartilhamento — A fase em que a informação é disponibilizada para uso através de um método de distribuição. As atividades nesta fase se referem aos processos de alocação da informação em locais onde ela possa ser acessada e usada para, por exemplo, distribuição de documentos por e-mail. Para a informação mantida eletronicamente, esta fase do ciclo de vida pode sobrepor-se em grande medida à fase de armazenamento, por exemplo, compartilhando da informação através de acesso ao banco de dados, servidores de arquivos/documentos.

- Uso — A fase em que a informação é usada para atingir os objetivos. As atividades nesta fase podem se referir a todos os tipos de uso de informação (por exemplo, tomada de decisão gerencial, processo automatizados de execução) e também podem incluir atividades como recuperação de informações e conversão de informações de um formato para outro.

De acordo com a visão do *Taking Governance Forward*, a informação é um habilitador de governança corporativa; por essa razão, o uso da informação conforme definição no IM pode ser pensado como a finalidade pela qual as partes interessadas responsáveis pela governança corporativa necessitam da informação ao assumirem seus papéis, realizar suas atividades e interagindo entre si.

Estas funções, atividades e relações são mostradas na figura 8. As interações entre as partes interessadas exigem fluxos de informações cujos objetivos são indicados no esquema: responsabilidade, delegação, monitoramento, definição da orientação, alinhamento, execução e controle.

Monitorar — A fase onde é assegurado que os recursos da informação continuarão funcionando adequadamente, ou seja, para terem valor. As atividades desta fase podem se referir à manutenção da atualização da informação bem como outros tipos de atividades de gerenciamento da informação tais como aperfeiçoamento, limpeza, mesclagem e remoção de dados duplicados dos *Data Warehouses*.

Descartar — A fase em que os recursos da informação são descartados quando já não têm mais utilidade. As atividades desta fase podem se referir ao arquivamento e destruição da informação.

- **Boas Práticas** — O conceito de informação é compreendido de forma diferente em distintas disciplinas tais como economia, teoria da comunicação, ciência da informação, gestão do conhecimento e sistemas da informação; portanto, não há uma definição consagrada mundialmente sobre no que consiste a informação. A natureza da informação pode, contudo, ser esclarecida através da definição e descrição de suas propriedades.

O seguinte esquema é proposto para estruturar as diferentes propriedades da informação: ele contém seis níveis ou camadas para definir e descrever as propriedades da informação. Esses seis níveis apresentam atributos contínuos, que variam desde o mundo físico da informação, onde os atributos se conectam com as tecnologias da informação e os meios para a captura, armazenamento, processamento, distribuição e apresentação da informação, até o mundo social do uso, compreensão e ação relacionados à informação.

As descrições abaixo podem ser atribuídas às camadas e atributos da informação:

- **Camada do mundo físico** — O mundo onde todos os fenômenos que podem ser empiricamente observados acontecem
  - Portador/mídia de informação — O atributo que identifica o portador físico da informação, por exemplo, papel, sinais elétricos, ondas sonoras
- **Camada empírica** — A observação empírica dos sinais usados para codificar a informação e suas distinções entre si e do ruído de fundo
  - Canal de acesso à informação — O atributo que identifica o canal de acesso da informação, por exemplo, interfaces de usuários
- **Camada sintática** — Regras e princípios para criação de sentenças em linguagens naturais ou artificiais. A sintaxe se refere à forma da informação.
  - Código/linguagem — Atributo que identifica a linguagem/formato representacional usado para codificar a informação e as regras para combinação dos símbolos da linguagem para formar estruturas sintáticas.
- **Camada semântica** — Regras e princípios para construção do significado a partir das estruturas sintáticas. Semântica se refere ao significado da informação.
  - Tipo de Informação — Atributo que identifica o tipo da informação, por exemplo, informação financeira ou não financeira, informação com origem interna ou externa, valores previstos/esperados ou observados, valores planejados ou realizados
  - Atualização da informação — Atributo que identifica a linha do tempo atribuída à informação, por exemplo, informação no passado, presente ou futuro
  - Nível da informação — Atributo que identifica o grau de detalhamento da informação, por exemplo, vendas anuais, trimestrais, mensais
- **Camada pragmática** — Regras e estruturas para construção de estruturas de linguagem mais amplas que atendam a finalidades específicas da comunicação humana. Pragmática se refere ao uso da informação.
  - Período de retenção — Atributo que identifica o tempo que a informação pode ser retida antes de ser destruída
  - Status da informação — Atributo que identifica se a informação é operacional ou histórica
  - Inovação — Atributo que identifica se a informação cria novo conhecimento ou confirma conhecimento já existente, por exemplo, informação ou confirmação
  - Contingência — Atributo que identifica as informações necessárias para preceder esta informação (para ela ser considerada uma informação)
- **Camada do mundo social** — O mundo construído socialmente pelo uso de estruturas de linguagem no nível pragmático da semiótica, por exemplo, contratos, legislação, cultura
  - Contexto — O atributo que identifica o contexto em que a informação faz sentido, é usada, tem valor, etc., por exemplo, contexto cultural, contexto de domínio de assunto

Considerações adicionais sobre a informação —Investimentos em informação e tecnologia correlata se baseiam nos estudos de caso, que incluem a análise do custo-benefício. Custos e benefícios não se referem somente a fatores tangíveis e mensuráveis, eles também consideram fatores intangíveis tais como vantagem competitiva, satisfação do cliente e incerteza

tecnológica. A organização gera benefícios a partir de tal análise somente após o recurso da informação ser aplicado ou utilizado, e desse modo o valor da informação é determinado exclusivamente através do seu uso (internamente ou pela sua venda) e a informação não tem valor intrínseco. O valor só pode ser gerado quando a informação é colocada em ação.

O IM é um novo modelo, muito valioso em termos de componentes diferentes. Ele ainda será desenvolvido em uma publicação separada. Para torna-lo mais tangível para o usuário do COBIT 5, e para deixar sua relevância mais clara no contexto do modelo geral do COBIT 5, são apresentados os exemplos 13, 14 e 15 com o possível uso do IM.

EXEMPLO 13 — MODELO DE INFORMAÇÃO USADO PARA AS ESPECIFICAÇÕES DA INFORMAÇÃO

Ao desenvolver um novo aplicativo, o IM pode ser usado para apoiar as especificações do aplicativo bem como informações correlatas ou os modelos de dados.

Os atributos de informação do IM podem ser usados para definir as especificações do aplicativo e dos processos de negócios que farão uso da informação.

Por exemplo, o projeto e as especificações de um novo sistema devem especificar:

- **Camada física** — Onde a informação será armazenada?
- **Camada empírica** — Como a informação pode ser acessada?
- **Camada sintática** — Como a informação será estruturada e codificada?
- **Camada semântica** — A informação é de que tipo? Qual é o nível da informação?
- **Camada pragmática** — Quais são os requisitos de retenção? Que outra informação é necessária para que esta informação seja útil e utilizável?

Observando a dimensão do interessado em combinação com o ciclo de vida da informação, é possível definir quem precisará de determinado tipo de acesso aos dados durante determinada fase do ciclo de vida da informação.

Quando o aplicativo é testado, os testadores podem observar os critérios de qualidade da informação para desenvolver um conjunto abrangente de casos de teste.

EXEMPLO 14 — MODELO DE INFORMAÇÃO USADO PARA DETERMINAR A PROTEÇÃO NECESSÁRIA

Grupos de segurança corporativa podem se beneficiar com a dimensão dos atributos do IM. De fato, quando incumbidos de proteger a informação, eles devem observar:

- **Camada física** — Como e onde a informação é fisicamente armazenada?
- **Camada empírica** — Quais são os canais de acesso à informação?
- **Camada semântica** — Qual o tipo de informação? A informação é atual ou se refere ao passado ou futuro?
- **Camada pragmática** — Quais são os requisitos de retenção? A informação é histórica ou operacional?

Ao utilizar estes atributos, o usuário poderá determinar o nível de proteção e os mecanismos de proteção necessários.

Observando a outra dimensão do IM, profissionais de segurança também podem considerar as fases do ciclo de vida da informação, visto que a informação deve ser protegida durante todas as fases do ciclo de vida. De fato, a segurança começa na fase de planejamento da informação, e implica diferentes mecanismos de proteção para armazenamento, compartilhamento e descarte da informação. O IM garante que a proteção da informação durante todo o seu ciclo de vida.

EXEMPLO 15 — MODELO DE INFORMAÇÃO USADO PARA DETERMINAR A FACILIDADE DE USO DOS DADOS

Ao analisar um processo de negócios (ou um aplicativo), o IM pode ser usado para auxiliar na análise geral das informações processadas e geradas pelo processo, e dos sistemas de informação subjacentes. Os critérios de qualidade podem ser usados para avaliar em que medida a informação é disponibilizada — se a informação é completa, disponibilizada em tempo hábil, factualmente correta, pertinente e disponibilizada na quantidade adequada. Também é possível considerar os critérios de acessibilidade — se a informação é acessível quando necessário e protegida adequadamente.

A análise também pode ser estendida para incluir critérios de representação, por exemplo, a facilidade com que a informação pode ser compreendida, interpretada, usada e manipulada.

A análise que usar os critérios de qualidade da informação do IM fornecerá à organização uma visão abrangente e completa sobre a atual qualidade da informação dentro de um processo de negócios.

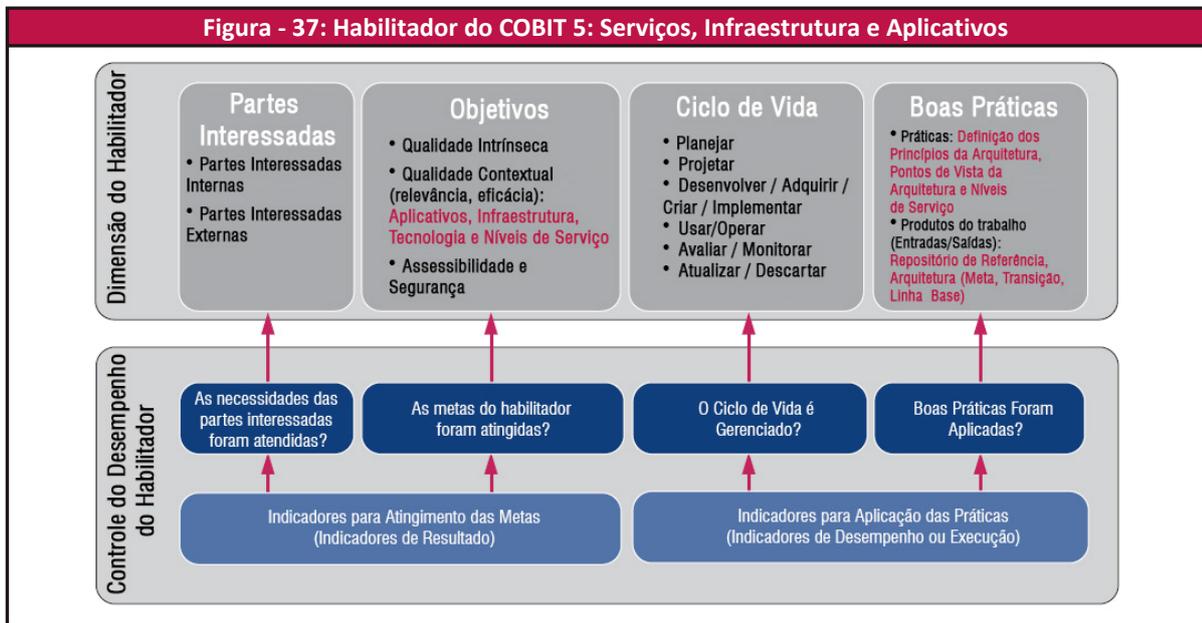
Habilitador COBIT 5: Serviços, Infraestrutura e Aplicativos

A capacidade de serviço se refere a recursos tais como aplicativos e infraestruturas alavancados na prestação dos serviços de TI.

As especificidades do habilitador capacidade de serviço são comparadas com a descrição do habilitador genérico e apresentadas na figura 37.

O modelo do habilitador serviços, infraestrutura e aplicativos destaca:

- **Partes interessadas** — Partes interessadas das capacidades de serviço (o termo combinado para serviços, infraestrutura e aplicativos), podem ser internas e externas. Os serviços podem ser prestados por partes internas ou externas — departamentos de TI internos, gerências operacionais, fornecedores terceirizados. Os usuários dos serviços também podem ser internos — usuários de negócios — e externos à organização — parceiros, clientes, fornecedores. Os interesses de cada parte interessada devem ser identificados e serão concentrados na prestação de serviços adequados ou no recebimento dos serviços solicitados pelos fornecedores.
- **Metas** — As metas de capacidade do nível de serviço serão expressas em termos de serviços — aplicativos, infraestrutura, tecnologia — e níveis de serviço, levando em consideração quais serviços e níveis de serviço são mais econômicos para a organização. Reiterando, as metas estarão relacionadas com os serviços e como eles são prestados, bem como seus resultados, por exemplo, contribuição com processos de negócios corretamente sustentados.
- **Ciclo de vida** — As capacidades de serviço possuem um ciclo de vida. As capacidades de serviço futuras ou planejadas são tipicamente descritas em uma arquitetura alvo. Elas cobrem os módulos, tais como aplicativos futuros e modelos de infraestrutura alvo, e ainda descrevem as conexões e relações entre estes módulos.

Figura - 37: Habilitador do COBIT 5: Serviços, Infraestrutura e Aplicativos

As atuais capacidades de serviço usadas ou operadas para prestar os atuais serviços de TI são descritas em uma arquitetura de referência. Dependendo do tempo de duração da arquitetura alvo, uma arquitetura de transição também pode ser definida, que mostra a evolução corporativa desde a arquitetura de referência até a arquitetura alvo.

- Boas práticas — As boas práticas das capacidades de serviço incluem:
  - Definição dos princípios de arquitetura — Princípios de arquitetura são diretrizes gerais que norteiam a implementação e o uso dos recursos de TI da organização. Exemplos de possíveis princípios de arquitetura são:
    - **Reaproveitamento** — Componentes comuns da arquitetura devem ser usados ao projetar e implementar soluções como parte das arquiteturas alvo ou de transição.
    - **Compra ou desenvolvimento** — As soluções devem ser compradas a menos que haja uma justificativa aprovada para seu desenvolvimento interno.
    - **Simplicidade** — A arquitetura corporativa deve ser projetada e mantida da forma mais simples possível e ainda atender aos requisitos da organização.
    - **Agilidade** — A arquitetura corporativa deve ser ágil para satisfazer as necessidades de mudança dos negócios de forma eficaz e eficiente.
    - **Abertura** — A arquitetura corporativa deve alavancar os padrões abertos do setor.
  - As definições da organização dos pontos de vista de arquitetura mais adequados deverão atender às necessidades de diferentes partes interessadas. Estes são os modelos, catálogos e matrizes usados para descrever as arquiteturas de referência, alvo ou de transição; por exemplo, a arquitetura de um aplicativo poderia ser descrita por meio de um diagrama de interface de aplicativo, que mostra os aplicativos em uso (ou planejados) e as interfaces entre eles.
  - Dispor de um arquivo de arquitetura, que pode ser usado para armazenar diferentes tipos de saídas arquitetônicas, inclusive princípios e padrões de arquitetura, modelos de referência de arquitetura bem como outros serviços de arquitetura, e que definam os módulos de serviço tais como:
    - Aplicativos, que proporcionam funcionalidade aos negócios

- Infraestrutura de tecnologia, inclusive hardware, software de sistema e infraestrutura de rede
  - Infraestrutura física
- Os níveis de serviço que devem ser definidos e alcançados pelos prestadores de serviços

Existem boas práticas para as estruturas de arquitetura e capacidades de serviço. São diretrizes, modelos ou padrões que poderiam ser usados para acelerar a criação dos serviços da arquitetura. Exemplos:

- TOGAF[16] fornece um Modelo de Referência Técnica e um Modelo Integrado de Referência da Infraestrutura da Informação.
- ITIL fornece ampla orientação sobre como conceber e operar os serviços.

- **Relações com outros habilitadores** — As interações com outros habilitadores incluem:
  - A informação é uma das capacidades de serviço e as capacidades de serviço são alavancadas pelos processos de prestação de serviços internos e externos.
  - Os aspectos culturais e comportamentais também são pertinentes quando uma cultura orientada ao serviço tiver de ser criada.
  - No COBIT 5, as entradas e saídas das práticas e atividades de gestão podem incluir capacidades de serviço, requeridas como entradas ou geradas como resultados.

[16] *www.opengroup.org/togaf*

Habilitador do COBIT 5: Pessoas, Habilidades e Competências

As especificidades do habilitador pessoas, habilidades e competências são comparadas com a descrição do habilitador genérico e apresentadas na figura 38.

Figura - 38: Habilitador do COBIT 5: Pessoas, Habilidades e Competências

Dimensão do Habilitador

Partes Interessadas
• Partes Interessadas Internas
• Partes Interessadas Externas

Objetivos
• Qualidade Intrínseca: Educação e Qualificações, Habilidades Técnicas
• Qualidade Contextual (relevância, eficácia): Experiência, Conhecimento, Habilidade Comportamental, Disponibilidade, Rotatividade
• Assessibilidade e Segurança

Ciclo de Vida
• Planejar
• Projetar
• Desenvolver / Adquirir / Criar / Implementar
• Usar/Operar
• Avaliar / Monitorar
• Atualizar / Descartar

Boas Práticas
• Práticas: Definição das Habilidades Exigidas para a Função, Níveis de Habilidades, Categorias de Habilidades
• Produtos do trabalho (Entradas/Saídas): Definição das Habilidades

Controle do Desempenho do Habilitador

As necessidades das partes interessadas foram atendidas?
As metas do habilitador foram atingidas?
O Ciclo de Vida é Gerenciado?
Boas Práticas Foram Aplicadas?

Indicadores para Atingimento das Metas (Indicadores de Resultado)
Indicadores para Aplicação das Práticas (Indicadores de Desempenho ou Execução)

O modelo do habilitador pessoas, habilidades e competências destaca:

- **Partes interessadas** — As habilidades e competências podem ser encontradas em Partes Interessadas internas e externas à organização. Cada interessado assume funções participantes — administradores de negócios, administradores de projeto, parceiros, concorrentes, recrutadores, instrutores, desenvolvedores, especialistas técnicos em TI, etc. — e cada papel exige um conjunto de habilidades distintas.
- **Metas** — As metas das habilidades e competências estão relacionadas com os níveis de educação e qualificação, habilidades técnicas, níveis de experiência, conhecimento e habilidades comportamentais necessários para realizar e desenvolver as atividades do processo com sucesso, os papéis organizacionais, etc. As metas dos funcionários incluem níveis corretos de disponibilidade de pessoal e índice de rotatividade.
- Ciclo de vida:
  - Habilidades e competências têm um ciclo de vida. Uma organização tem que saber qual é sua atual base de habilidades e planejar o que ela deve ser. Isto é influenciado pela estratégia (entre outras coisas) e pelos objetivos corporativos. As habilidades devem ser desenvolvidas (por exemplo, com treinamento) ou adquiridas (por exemplo, com recrutamento) e implantadas nos diversos papéis da estrutura organizacional. As habilidades devem ser transferidas, por exemplo, se uma atividade for automatizada ou terceirizada.
  - Periodicamente, por exemplo, anualmente, a organização deve avaliar a base de competências para compreender a evolução ocorrida, que será informada no processo de planejamento do próximo período.
  - Esta avaliação também pode ser incluída no processo de recompensa e reconhecimento de recursos humanos.
- Boas práticas:
  - As boas práticas de habilidades e competências incluem a definição de requisitos de qualificação claros e objetivos de cada papel desempenhado pelas diversas partes interessadas. Isto pode ser descrito em diferentes níveis de habilidades em diversas categorias. Para cada nível de habilidade apropriado em cada categoria de habilidade, uma definição da habilidade deverá ser disponibilizada. As categorias de habilidade correspondem às atividades de TI assumidas, por exemplo, gestão da informação, análise de negócios.
  - Outras boas práticas:
    - Há fontes externas de boas práticas, como *Skills Framework for the Information Age* (SFIA),[17] que fornece definições detalhadas de habilidades.
    - Exemplos de potenciais categorias de habilidades, mapeados nos domínios de processo do COBIT 5 são apresentados na figura 39.

Figura - 39: Categorias de Habilidades do COBIT 5	
Domínio do Processo	Exemplos de Categorias de Habilidades
Avaliar, Dirigir e Monitorar (EDM)	• Governança corporativa de TI
Alinhar, Planejar e Organizar (APO)	• Formulação da política de TI • Estratégia de TI • Arquitetura corporativa • Inovação • Gestão financeira • Gestão de portfólio
Construir, Adquirir e Implementar (BAI)	• Análise de negócios • Gerenciamento de projetos • Avaliação de usabilidade • Definição e gestão de requisitos • Programação • Ergonomia do sistema • Desativação de software • Gestão da capacidade
Entregar, Serviços e Suporte (DSS)	• Gestão da disponibilidade • Gestão de problemas • Central de Atendimento e gestão de incidentes • Administração de segurança • Operações de TI • Administração do banco de dados
Monitorar, Avaliar e Analisar (MEA)	• Análise de conformidade • Monitoramento de desempenho • Auditoria de controles

- **Relações com outros habilitadores** — As interações com outros habilitadores incluem:
  - Habilidades e competências são necessárias para realizar as atividades do processo e tomar decisões em estruturas organizacionais. Reciprocamente, alguns processos visam apoiar o ciclo de vida das habilidades e competências.
  - Há ainda uma relação com a cultura, ética e comportamento através das habilidades comportamentais, que orientam o comportamento do indivíduo e são influenciadas pela ética da pessoa e pela ética da organização.
  - As definições de habilidades também são informações, para as quais boas práticas do habilitador de informação devem ser consideradas.

APÊNDICE H
GLOSSÁRIO

TERMO	DEFINIÇÃO
Alinhamento	O estado em que os habilitadores de governança e gestão de TI da organização apoiam os objetivos e estratégias da organização
Aplicativo de TI	Funcionalidade eletrônica que faz parte dos processos de negócios assumidos por TI ou com a sua assistência
Aprovador	Pessoa ou grupo que detém ou possui os direitos e as responsabilidades em relação a uma organização, entidade ou ativo, por exemplo, responsável pelo processo, responsável pelo sistema
Arquitetura de aplicativo	Descrição do agrupamento lógico das capacidades que controlam os objetos necessários para processamento da informação e apoio aos objetivos corporativos
Arquitetura de referência	A atual descrição do projeto básico subjacente dos componentes do sistema de negócios antes de entrar em um ciclo de análise e novo projeto de arquitetura
Atividade	No COBIT, a principal ação tomada para operar o processo. Orientação para cumprir as práticas de administração visando êxito na governança e gestão de TI da organização. As atividades: • Descrevem um conjunto de etapas de implementação orientadas à ação necessárias e suficientes para atingir a Prática de Governança ou a Prática de gestão • Consideraram as entradas e saídas do processo • Têm como base os padrões e boas práticas geralmente aceitos • Apoiam a criação de funções e responsabilidades bem definidas • Não são prescritivas e devem ser adaptadas e desenvolvidas em procedimentos específicos adequados à organização
Atributo (de capacidade) do processo	ISO/IEC 15504: Uma característica mensurável da capacidade do processo aplicável a qualquer processo
Autenticação	O ato de verificar a identidade de um usuário e a qualificação do usuário para acesso às informações computadorizadas Nota sobre o Escopo: Garantia: O objetivo da autenticação é oferecer proteção contra atividades de *logon* (acesso) fraudulento. Ela também pode se referir à verificação da exatidão de um dado
Alinhamento	O estado em que os habilitadores de governança e gestão de TI da organização apoiam os objetivos e estratégias da organização
Aplicativo de TI	Funcionalidade eletrônica que faz parte dos processos de negócios assumidos por TI ou com a sua assistência
Boas práticas	Atividade ou processo comprovado que tem sido aplicado com sucesso por diversas organizações e tem sido apresentado para produzir resultados confiáveis
Capacidade do processo	ISO/IEC 15504: Uma caracterização da capacidade de um processo de cumprir os objetivos do negócio, atuais ou projetados
Catálogo de serviços	Informação estruturada sobre todos os serviços de TI disponíveis aos clientes
Ciclo de vida econômico	O período durante o qual se espera a realização de benefícios substanciais para a organização e/ou durante o qual se espera a inocorrência de despesas substanciais (inclusive investimentos, custos com execução e aposentadoria) por um programa de investimento
COBIT	1. COBIT 5: Conhecido antigamente como *Control Objectives for Information and related Technology* [Objetivos de Controle da Informação e Tecnologia relacionada] (COBIT); agora apresentado somente como uma sigla em sua quinta iteração. Uma estrutura completa, aceita internacionalmente, para governança e gestão da tecnologia e informação (TI) da organização que apoia os executivos e a administração da organização na definição e consecução dos objetivos do seu negócio e dos objetivos de TI. O COBIT descreve cinco princípios e sete habilitadores que apoiam as organizações no desenvolvimento, implementação, melhoria e monitoramento contínuos das boas práticas de governança e gestão de TI Nota sobre o Escopo: Versões anteriores do COBIT se concentravam nos objetivos de controle dos processos de TI, gestão e controle de processos de TI e aspectos de governança de TI. A adoção e o uso da estrutura do COBIT são apoiados pela orientação de uma crescente família de produtos de suporte (Ver *www.isaca.org/cobit* para mais informações)

TERMO	DEFINIÇÃO
	2. COBIT 4.1 e versões anteriores: Conhecidos antigamente como *Control Objectives for Information and related Technology* [Objetivos de Controle da Informação e Tecnologia relacionada] (COBIT). Uma estrutura completa de processos de TI, aceita internacionalmente, que apoia os executivos de negócios e de TI bem como a administração na definição e consecução dos objetivos do seu negócio e dos objetivos de TI, fornecendo um modelo abrangente de governança, administração, controle e garantia de TI. O COBIT descreve os processos de TI e os respectivos objetivos de controle, diretrizes de gestão (atividades, responsabilidades e métricas de desempenho) além de modelos de maturidade. O COBIT apoia a administração da organização no desenvolvimento, implementação, melhoria e monitoramento contínuos das boas práticas de TI Nota sobre o escopo: A adoção e o uso da estrutura do COBIT são apoiados por orientações para executivos e para a administração (*Board Briefing on IT Governance*, *2nd Edition*), implementadores da governança de TI (COBIT *Quickstart, 2nd Edition*; *IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition*; e *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance*), e profissionais de garantia e auditoria de TI (*IT Assurance Guide Using COBIT*). Também há orientação para apoiar sua aplicabilidade a determinadas exigências legais e regulatórias (por exemplo*, IT Control Objectives for Sarbanes-Oxley, IT Control Objectives for Basel II*) bem como sua relevância para a segurança da informação (*COBIT Security Ba*seline). COBIT é mapeado em outras modelo e padrões para ilustrar a cobertura completa do ciclo de vida da gestão de TI e apoiar seu uso pelas organizações com o uso de múltiplos padrões e modelo de TI
Cobrança retroativa	A redistribuição das despesas às unidades de uma organização que lhes deram origem
Código de Ética	Documento elaborado para influenciar o comportamento individual e organizacional dos funcionários definindo valores organizacionais e as regras a serem aplicadas em determinadas situações. Ele é adotado para auxiliar os responsáveis pela tomada de decisões da organização a entender a diferença entre "certo" e "errado" e aplicar este entendimento em suas decisões
Competência	A habilidade de realizar uma tarefa, ação ou função específica com sucesso
Conselho de arquitetura	Um grupo de participantes e especialistas responsáveis pela orientação nos assuntos e decisões relacionados à arquitetura corporativa e pela definição das políticas e padrões de arquitetura
Contexto	O conjunto completo de fatores internos e externos que podem influenciar ou determinar como uma organização, entidade, processo ou indivíduo se comporta Nota sobre o Escopo: O contexto inclui: • Contexto tecnológico – Fatores tecnológicos que afetam a habilidade de uma organização de capturar valor dos dados • Contexto dos dados – Exatidão, disponibilidade, atualização e qualidade dos dados • Habilidades e conhecimento – Experiência geral e habilidades analíticas, técnicas e corporativas • Contexto cultural e organizacional– Fatores políticos, e se a organização prefere dados a intuição • Contexto estratégico – Objetivos estratégicos da organização
Continuidade do negócio	Prevenção, mitigação e recuperação após uma interrupção. Os termos "planejamento de restabelecimento de negócios", "planejamento de recuperação de desastres" e "planejamento de contingência" também podem ser usados neste contexto; eles se concentram nos aspectos de recuperação da continuidade, e por esse motivo o aspecto "resiliência" também deve ser considerado
Controle	Os meios para gerenciar os riscos, inclusive políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, ou jurídica. Também usado como sinônimo de salvaguarda ou contramedida
Controle do processo de negócios	As políticas, procedimentos, práticas e estruturas organizacionais projetadas para fornecer garantia razoável de que um processo de negócios alcançará seus objetivos
Criação de valor	O principal objetivo da governança de uma organização, atingido quando os três objetivos subjacentes
Cultura	Um padrão de comportamentos, convicções, assunções, atitudes e formas de fazer as coisas
Entradas e saídas	Os produtos do trabalho/artefatos do processo considerados necessários para apoiar a operação do processo. Eles facilitam decisões importantes, fornecem um registro e uma prova de auditoria das atividades do processo e permitem o acompanhamento no caso de incidentes. São definidos no principal nível da prática de gestão, podem incluir alguns produtos do trabalho usados somente no processo e frequentemente são entradas críticas

TERMO	DEFINIÇÃO
	para outros processos. A ilustração de "entradas e saídas do COBIT 5" não deve ser considerada uma lista completa e definitiva uma vez que novos fluxos de informações podem ser definidos dependendo do ambiente e da estrutura do processo de uma organização específica
Estrutura de governança	Estrutura é um conceito básico usado para resolver ou abordar assuntos complexos; um habilitador de governança; um conjunto de conceitos, assunções e práticas que definem como algo pode ser abordado ou entendido, as relações entre as entidades envolvidas, as funções dos evolvidos e os limites (o que é ou não incluído no sistema de governança) Exemplos: COBIT e *COSO's Internal Control — Integrated Framework*
Estrutura organizacional	Um habilitador de governança e gestão. Inclui a organização e suas estruturas, hierarquias e dependências Exemplo: Comitê diretor
Gestão	Implica o uso ponderado dos meios (recursos, pessoas, processos, práticas, etc.) para atingir um determinado objetivo. É o meio ou instrumento pelo qual o órgão de governança alcança um resultado ou objetivo. A gestão é responsável pela execução da orientação definida pelo órgão de governança. Gestão diz respeito ao alinhamento das atividades de planejamento, desenvolvimento, organização e controle operacional com a orientação definida pelo órgão de governança, e à geração de relatórios sobre essas atividades
Gestão de riscos	Um dos objetivos da governança. Implica o reconhecimento do risco; avaliação do impacto e da probabilidade daquele risco; e desenvolvimento de estratégias para evitar o risco, reduzir o efeito negativo do risco e/ou transferir o risco, para administrá-lo no contexto da organização de inclinação ao risco.
Governança	A estrutura, princípios e políticas, modelo, processos e práticas, informação, habilidades, cultura, ética e comportamento para determinar a orientação e monitorar a conformidade e o desempenho da organização em consonância com o propósito geral e os objetivos definidos. A governança define a responsabilidade e tomada de decisões (entre outros elementos)
Governança corporativa	Um conjunto de responsabilidades e práticas exercidas pelo conselho e pela gestão executiva com o objetivo de fornecer orientação estratégica, garantindo que os objetivos sejam alcançados, considerando a gestão de riscos adequada e verificando se os recursos da organização são utilizados com responsabilidade. Também poderia significar uma visão de governança concentrada na organização como um todo; a visão da governança em seu nível mais alto e à qual todos os demais devem se alinhar
Governança Corporativa de TI	Uma visão de governança que garante que a informação e a tecnologia relacionada apoiem e possibilitem a estratégia da organização e a consecução dos objetivos corporativos. Também inclui a governança funcional de TI, ou seja, garantindo que as capacidades de TI sejam fornecidas com eficiência e eficácia
Habilidade	A capacidade adquirida para atingir resultados predeterminados
Habilitador de governança	Algo (tangível ou intangível) que auxilia na realização da governança efetiva. (O Tribunal de Contas da União (TCU) e entidades do governo usam também o termo "Viabilizador". Os dois termos são aceitos como corretos "Habilitador de governança" ou "Viabilizador de governança")
Informação	Um ativo, assim como outros ativos importantes da organização, crítico para os negócios da organização. Ela pode existir em muitas formas: impressa ou escrita em papel, armazenada eletronicamente, enviada pelo correio e por um meio eletrônico, apresentada em filmes ou ainda divulgada em conversas
Interessado	Qualquer pessoa responsável por uma expectativa ou qualquer outro interesse da organização – por exemplo, participantes, usuários, governo, fornecedores, clientes e o público
Métrica	Entidade quantificável que permite a medição da consecução de um objetivo do processo. As métricas devem ser SMART – específicas, mensuráveis, acionáveis, pertinentes e tempestivas. A orientação completa das métricas define a unidade utilizada, a frequência de medição, valor-alvo ideal (se for o caso) bem como o procedimento para fazer a medição e o procedimento para interpretação da avaliação
Modelo	Uma forma de descrever um determinado conjunto de componentes e como estes componentes se relacionam entre si para descrever as principais funções de um objeto, sistema ou conceito
Objetivo	Declaração do resultado esperado
Objetivo corporativo	Ver Objetivo do negócio

TERMO	DEFINIÇÃO
Objetivo de TI	Declaração que descreve o resultado de TI esperado pela organização em apoio aos objetivos corporativos. O resultado pode ser um artefato, uma mudança significativa de um estado ou o aumento significativo da capacidade
Objetivo do negócio	A tradução da missão da organização, expressa em uma declaração de intenção, em metas de desempenho e resultados
Objetivo do processo	Declaração que descreve o resultado esperado de um processo. O resultado pode ser um artefato, uma mudança de estado significativa ou o aumento significativo da capacidade de outros processos
Órgão Gestor de Programas e Projetos (PMO)	Função responsável por apoiar os gerentes de programas e projetos e reunir, avaliar e reportar a informação por meio de relatório sobre a conduta de seus programas e dos projetos que os compõem
Otimização de recursos	Um dos objetivos da governança. Envolve o uso eficaz, eficiente e responsável de todos os recursos humanos, financeiros, equipamentos, instalações, etc.
Parte consultada (RACI)	Refere-se àquelas pessoas cujas opiniões são solicitadas em uma atividade (comunicação bidirecional) Em uma tabela RACI, responde à pergunta: Quem é responsável pelas entradas? As principais funções que fornecem entrada. Observe que também fica a critério das funções responsáveis obterem as informações junto a outras unidades ou parceiros externos; no entanto, as entradas provenientes das funções relacionadas serão consideradas e, se necessário, ações adequadas deverão ser tomadas para escalação, inclusive a informação do responsável pelo processo e/ou do comitê diretor
Parte informada (RACI) (Informed)	Refere-se às pessoas mantidas informadas e atualizadas sobre o andamento de uma atividade (comunicação unidirecional) Em uma tabela RACI, responde à pergunta: Quem recebe a informação? As funções informadas sobre a consecução e/ou resultados da tarefa. A função de “responsável”, evidentemente, sempre deverá receber informação adequada para supervisionar a tarefa, da mesma forma que as funções responsáveis por sua área de interesse
Parte Aprovadora (RACI) (Accountable)	Pessoa, grupo ou entidade responsável basicamente por um assunto, processo ou escopo Em uma tabela RACI, responde à pergunta: Quem responde pelo sucesso da tarefa?
Parte Responsável (RACI) (Responsible)	Refere-se à pessoa que deve garantir que as atividades sejam concluídas com sucesso Em uma tabela RACI, responde à pergunta: Quem está realizando a tarefa? As funções que tiverem o principal interesse operacional na realização da atividade relacionada e criarem o resultado esperado
Política	Intenção e orientação gerais conforme formalmente expressas pela administração
Portfólio de investimentos	O conjunto de investimentos sendo considerados e/ou realizados
Prática de governança/gestão	Para cada processo do COBIT, as práticas de governança e gestão fornecem um conjunto completo de requisitos em alto nível para a prática e eficiente governança e gestão de TI da organização. Elas são declarações de ações para os órgãos de governança e para a administração
Princípio	Um habilitador de governança e de gestão. Ele inclui os valores e assunções fundamentais adotados pela organização, as convicções que orientam e impõem limites à tomada de decisão da organização, a comunicação dentro e fora da organização bem como a administração – gestão de ativos de terceiros Exemplo: Código de ética, Estatuto de responsabilidade social
Processo	Via de regra, um conjunto de práticas influenciadas pelas políticas e procedimentos da organização, alimentado por diversas fontes (inclusive outros processos), que manipula as entradas e produz saídas (por exemplo, produtos, serviços) Nota sobre o Escopo: Processos têm propósitos corporativos claramente definidos para existir, responsáveis, funções e responsabilidades bem definidos para execução do processo, bem como os meios para medir o desempenho
Qualidade	Ser adequado ao objetivo (criar o valor esperado)
Realização dos benefícios	Um dos objetivos da governança. A interposição de novos benefícios para a organização, manutenção e ampliação de das atuais formas de benefícios e a eliminação daquelas iniciativas e ativos que não criam o valor esperado
Recursos	Qualquer ativo da organização que pode ajudá-la a atingir seus objetivos
Responsabilidade pela Governança	A governança garante que os objetivos corporativos sejam alcançados avaliando as necessidades, condições e opções das partes interessadas; definindo a orientação através

TERMO	DEFINIÇÃO
	da priorização e tomada de decisão; e monitorando o desempenho, conformidade e evolução dos planos. Na maioria das organizações, a governança é de responsabilidade do conselho de administração, sob a liderança do presidente
Risco	A combinação da probabilidade de um evento e suas consequências (ISO/IEC 73)
Saída	Ver Entradas e Saídas
Serviço de TI	O fornecimento diário aos clientes de infraestrutura e aplicativos de TI e suporte para seu uso. Exemplos incluem central de atendimento, fornecimento e mudança de equipamentos, bem como autorizações de segurança
Serviços	Ver Serviço de TI
Sistema de controle interno	Políticas, padrões, planejamentos e procedimentos, e estruturas organizacionais projetadas para fornecer a garantia razoável de que os objetivos corporativos serão atingidos e eventos indesejados serão evitados ou detectados e corrigidos
Tabela RACI	Ilustra quem é a pessoa Responsável, Aprovador, Consultada ou Informada dentro da estrutura organizacional
Tendência	Fatores internos e externos que desencadeiam e influenciam a forma como a organização ou as pessoas agem ou mudam